This publication was created by the members of the Institute of Law and Technology (Faculty of Law, Masaryk University).

Graphic design of the cover Petr Šavelka

This edition © Tribun EU, s. r. o.

## Contents – summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>E-Commerce and Consumer protection</td>
<td>9</td>
</tr>
<tr>
<td>II.</td>
<td>Competition Law</td>
<td>66</td>
</tr>
<tr>
<td>III.</td>
<td>Law of domain names</td>
<td>71</td>
</tr>
<tr>
<td>IV.</td>
<td>Public Sector Information</td>
<td>104</td>
</tr>
<tr>
<td>V.</td>
<td>ISP Liability</td>
<td>116</td>
</tr>
<tr>
<td>VI.</td>
<td>Cybercrime and Cybersecurity</td>
<td>136</td>
</tr>
<tr>
<td>VII.</td>
<td>Copyright Law</td>
<td>209</td>
</tr>
<tr>
<td>VIII.</td>
<td>Electronic documents</td>
<td>254</td>
</tr>
<tr>
<td>IX.</td>
<td>Data protection</td>
<td>280</td>
</tr>
<tr>
<td>X.</td>
<td>E-Finance</td>
<td>349</td>
</tr>
<tr>
<td>XI.</td>
<td>Jurisdiction</td>
<td>410</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Contents – summary</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. E-Commerce and Consumer protection</strong></td>
<td>9</td>
</tr>
<tr>
<td>Treaty on the functioning of the European Union (relevant provisions)</td>
<td>9</td>
</tr>
<tr>
<td>PART ONE – PRINCIPLES</td>
<td>9</td>
</tr>
<tr>
<td>PART THREE - TITLE II FREE MOVEMENT OF GOODS</td>
<td>11</td>
</tr>
<tr>
<td>PART THREE - TITLE IV FREE MOVEMENT OF PERSONS, SERVICES AND CAPITAL</td>
<td>11</td>
</tr>
<tr>
<td>TITLE XV CONSUMER PROTECTION</td>
<td>13</td>
</tr>
<tr>
<td>Relevant Case-Law on free movement of goods and services (on-line)</td>
<td>13</td>
</tr>
<tr>
<td>Case C-322/01, Deutscher Apotheker verband eV and 0800 DocMorris NV</td>
<td>13</td>
</tr>
<tr>
<td>Case C-243/01 Criminal proceedings against Piergiorgio Gambelli and Others</td>
<td>14</td>
</tr>
<tr>
<td>Case C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International Ltd, formerly Baw International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa</td>
<td>14</td>
</tr>
<tr>
<td>Case C-156/13, Digibet Ltd, Gert Albers v Westdeutsche Lotterie GmbH &amp; Co. OHG</td>
<td>14</td>
</tr>
<tr>
<td>Relevant case law on unfair terms in consumer contracts</td>
<td>44</td>
</tr>
<tr>
<td>Case C- 243/08, Pannon GSM Zrt. v Erzsébet Sustikné Győrfi</td>
<td>45</td>
</tr>
<tr>
<td>Relevant Case Law on Directive 2000/31/EC on electronic commerce</td>
<td>54</td>
</tr>
<tr>
<td>Case C- 244/06, Dynamic Medien Vertriebs GmbH v Avides Media AG, THE COURT (Third Chamber)</td>
<td>54</td>
</tr>
<tr>
<td>Case C- 298/07, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG</td>
<td>55</td>
</tr>
<tr>
<td>Case C - 292/10, G v Cornelius de Visser</td>
<td>55</td>
</tr>
<tr>
<td>Case C - 291/13 Soliris Papasavvas v O Filelefferos Dimosia Etainia Ltd, Takis Kounnafi, Giorgos Sertis</td>
<td>55</td>
</tr>
<tr>
<td>Relevant Case Law on Unfair Commercial Practices Directive</td>
<td>64</td>
</tr>
<tr>
<td>Case C - 122/10, Konsumentombudsmannen v Ving Sverige AB</td>
<td>64</td>
</tr>
<tr>
<td>Case C-657/11, Belgian Electronic Sorting Technology NV v Bert Pellaers, Visys NV</td>
<td>64</td>
</tr>
<tr>
<td><strong>II. Competition Law</strong></td>
<td>66</td>
</tr>
<tr>
<td>Treaty on the Functioning of the European Union (101 – 109)</td>
<td>66</td>
</tr>
<tr>
<td>CHAPTER 1: RULES ON COMPETITION</td>
<td>66</td>
</tr>
<tr>
<td>SECTION 1: RULES APPLYING TO UNDERTAKINGS</td>
<td>66</td>
</tr>
<tr>
<td>SECTION 2: AIDS GRANTED BY STATES</td>
<td>67</td>
</tr>
<tr>
<td>Relevant case-law to the Treaty on the Functioning of the EU Art 101-102</td>
<td>68</td>
</tr>
</tbody>
</table>
III. Law of domain names

Uniform Domain Name Dispute Resolution Policy ................................................................. 71
Rules for Uniform Domain Name Dispute Resolution Policy ..................................................... 71
Uniform Domain Name Resolution Policy – Relevant Case Law .................................................. 73
  America Online, Inc. v. Johuathan Investments, Inc., and AOLLNEWS.COM Case No. D 2001-0918 ........ 77
  Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale Case No. D2000-0662 ....................... 80
  FC Bayern München AG v. Peoples Net Services Ltd. Case No. D2003-0464 ............................... 82
  Dr. Michael Crichton v. In Stealth Mode Case No: D2002-0874 ............................................... 84
Regulation (EC) No 733/2002 of the European Parliament and of the council of 22 April 2002 on the implementation of the .eu Top Level Domain .................................................................................................................. 91
Commission regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration .............................................. 94
Relevant “Anti-cybersquatting” provisions of the U.S. Code .......................................................... 101

IV. Public Sector Information ..................................................................................................... 104
Relevant Case Law on Public Sector Information ......................................................................... 109
  Case C - 343/95, Diego Cali & Figli Srl v. Servizi Ecologici Porto di Genova SpA (SEPG) .................. 109
  Case C - 7/13, Creditinfo Länstaustrast hf. and Registers Iceland and the Icelandic State ............. 110
  Case C - 117/13, Technische Universität Darmstadt v Eugen Ulmer KG ........................................ 112

V. ISP Liability .......................................................................................................................... 116
Convention on Information and Legal Co-operation concerning "Information Society Services" ................................................................. 116
Relevant Case law concerning directive 2000/31/EC ................................................................ 127
  Case C - 324/09, L’Oréal SA and others v. eBay International AG and others .................................. 127
  Joined Cases C-236/08 to C-238/08: Google France SARL, Google Inc. vs. Louis Vuitton Malletier SA (C-236/08), Google France SARL vs. Viaticum SA, Lutecei SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08) .................................................. 129
  Case C - 314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH .................................................. 130
  Case of Delfi AS v. Estonia (ECHR Application No. 64569/09) .................................................... 131

VI. Cybercrime and Cybersecurity ............................................................................................ 136
Convention on Cybercrime ........................................................................................................ 136
Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ........................................... 146
Constitution on Cybercrime – Explanatory report ................................................................. 148
98/560/EC: Council Recommendation on the development of the competitiveness of the European audiovisual and
information services industry .................................................................................................. 178
Information Security Agency .................................................................................................. 182
Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems .................. 189
ANNEX I Requirements and tasks of the Computer Emergency Response Team (CERT) ........................................... 197
ANNEX II List of market operators .......................................................................................... 198
EXPLANATORY MEMORANDUM  DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning
measures to ensure a high common level of network and information security across the Union .......................... 198
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace ................................. 202

VII. Copyright Law ...................................................................................................................... 209
Berne Convention for the Protection of Literary and Artistic Works ............................................................. 209
Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations ........ 215
WIPO Copyright Treaty ............................................................................................................ 220
WIPO Performances and Phonograms Treaty ..................................................................................... 222
and related rights in the information society .................................................................................. 226

Relevant Case-Law on Directive 2001/29/EC .............................................................................. 233
C-5/08 Infoqip International A/S v Danske Dagblades Forening .............................................................. 233
C-462/09 Stichting de Thuiskopie v Opus Supplies Deutschland GmbH and Others ........................................... 233
C-467/08 Padawan v SGAE .......................................................................................................... 233
C-145/10 Eva-Maria Painer v Standard VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, Spiegel-Verlag Rudolf
Austein GmbH & Co KG, Verlag M. DuMont Schauberg Expedition der Kölnerischen Zeitung GmbH & Co KG .......... 233
C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) v Netlog NV ..................... 234
C-277/10 Martin Luksan v Petrus van der Let .................................................................................... 234
C-351/12 OSA – Ochranný svaz autorský pro práva k dílům hudebním o.s. v Léčebné lázně Mariánské Lázně a.s. .... 234
C-435/12 ACI Adam BV and Others v Stichting de Thuiskopie, Stichting Onderhandelingen Thuiskopie vergoeding .... 235
C-360/13 Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and Others ............... 235
C-463/12 Copydan Båndkopi proti Nokia Danmark A/S ........................................................................ 235
C-466/12 Nils Svensson and Others v Retriever Sverige AB ....................................................................... 236
C-117/13 Technische Universität Darmstadt v Eugen Ulmer KG ...................................................................... 236
C-201/13 Johan Deckmyn, Vrijheidsfonds VZW v Helena Vandersteen and others ........................................... 236
C-419/13 Art & Allposters International BV v Stichting Pictoright .................................................................. 236

Directive 2009/24/EC on the legal protection of computer programs ......................................................... 236

Relevant Case-Law on Directive 2009/24/EC .................................................................................. 239
C-393/09 Bezpečnostní softwarová asociace – Svaz softwarové ochrany v Ministerstvo Kultury ......................... 239
C-406/10 SAS Institute Inc. v World Programming Ltd ............................................................................. 239
C-128/11 UsedSoft GmbH v Oracle International Corp ............................................................................. 239


Relevant Case-Law on Directive 96/9/EC ...................................................................................... 244
C-203/02 The British Horseracing Board Ltd and Others v William Hill Organization Ltd ................................. 244
C-444/02 Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairoU AE (OPAP) .............................. 245

Institute of Law and Technology
Masaryk University, Faculty of Law


VIII. Electronic documents .............................................................................................................. 254


IX. Data protection .......................................................................................................................... 280

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 280

Charter of Fundamental Rights of the European Union (2007/C 303/01) .......................................................... 282

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data .......................................................................................................................... 283

Relevant Case Law on Convention for the Protection of Human Rights and Fundamental Freedoms .......................................................................................................................... 286

CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71) .......................................................... 286

CASE OF MALONE v. THE UNITED KINGDOM (Application no. 8691/79) .......................................................... 296

CASE OF NIEMIETZ v. GERMANY (Application no. 13710/88) .......................................................... 308

CASE OF ROTARU v. ROMANIA (Application no. 28341/95) .......................................................... 312

COPLAND v. THE UNITED KINGDOM (Application no. 62617/00) .......................................................... 319

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data .......................................................................................................................... 323


Relevant Case Law on the Directives 95/46/EC; 2002/58/EC .......................................................................................................................... 345

Case C-101/01 Criminal proceedings against Bodil Linqvist) .......................................................................................................................... 345

Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU .......................................................................................................................... 346

Case C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH .......................................................................................................................... 346

Case C-461/10 Bonnier Audio AB et al. v Perfect Communication Sweden AB .......................................................................................................................... 346

Joined Cases C-293/12 and C-594/12, (Digital Rights Ireland Ltd, Kärntner Landesregierung) .......................................................................................................................... 347

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González .......................................................................................................................... 347

Case C-212/13, František Ryněk v Úřad pro ochranu osobních údajů .......................................................................................................................... 348
X. E-Finance

Treaty on the functioning of the European Union (relevant provisions on free movement of persons, services and capital, euro currency and European Central Bank connected with E-Finance) ................................................................. 349


Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features ................................................................. 377

Relevant EU Regulations and Directive on European Union Supervisory Bodies ................................................................. 388

Relevant Case Law on Distant Marketing in Investments ................................................................. C-384/93 Alpine Investments v. Minister van Financiën (Minister for Finance) ................................................................. 388

Relevant Case-Law on Online Betting and Online Games of Chance ................................................................. 391

C-258/08 Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator ................................................................. 391

Relevant Case-Law on Payment Instruments and Payment Cards ................................................................. 395


Relevant Case-Law on Anti-Money Laundering ................................................................. 398

Joined cases C-478/11 P to C-482/11 P — Laurent Gbagbo (C-478/11 P), Katinan Justin Koné (C-479/11 P), Akissi Danièle Boni-Claiverie (C-480/11 P), Alcide Djédjé (C-481/11 P) and Affi Pascal N’Guessan (C-482/11 P) v Council of the European Union ................................................................. 398

C-212/11, Jyske Bank Gibraltar Ltd v Administración del Estado ................................................................. 402

XI. Jurisdiction

Council regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) — ................................................................. 410

Relevant Case Law on the repealed council regulation no 44/2001 ................................................................. 420

Case C-478/12 Maletic ................................................................. 420

Joined Cases C-509/09 and C-161/10 eDate Advertising GmbH v X, Olivier Martinez, Robert Martinez v MGN Limited ................................................................. 420

Joined Cases C-585/08 and C-144/09, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09), ................................................................. 420

Case C-523/10, Wintersteiger AG v Products 4U Sondermaschinenbau GmbH ................................................................. 421

Case C-170/12, Peter Pinckney v KDG Mediatech AG ................................................................. 421

Case C-190/11, Daniela Mühleitner v Ahmad Yusufi, Wadat Yusufi, ................................................................. 421


Regulation (EC) No 864/2007 of the European parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) ................................................................. 441
I. E-Commerce and Consumer protection

Treaty on the functioning of the European Union (relevant provisions)

PART ONE – PRINCIPLES

Article 1

1. This Treaty organises the functioning of the Union and determines the areas of, delimitation of, and arrangements for exercising its competences.

2. This Treaty and the Treaty on European Union constitute the Treaties on which the Union is founded. These two Treaties, which have the same legal value, shall be referred to as “the Treaties”.

TITLE I CATEGORIES AND AREAS OF UNION COMPETENCE

Article 2

1. When the Treaties confer on the Union exclusive competence in a specific area, only the Union may legislate and adopt legally binding acts, the Member States being able to do so themselves only if so empowered by the Union or for the implementation of Union acts.

2. When the Treaties confer on the Union a competence shared with the Member States in a specific area, the Union and the Member States may legislate and adopt legally binding acts in that area. The Member States shall exercise their competence to the extent that the Union has not exercised its competence. The Member States shall again exercise their competence to the extent that the Union has decided to cease exercising its competence.

3. The Member States shall coordinate their economic and employment policies within arrangements as determined by this Treaty, which the Union shall have competence to provide.

4. The Union shall have competence, in accordance with the provisions of the Treaty on European Union, to define and implement a common foreign and security policy, including the progressive framing of a common defence policy.

5. In certain areas and under the conditions laid down in the Treaties, the Union shall have competence to carry out actions to support, coordinate or supplement the actions of the Member States, without thereby superseding their competence in these areas. Legally binding acts of the Union adopted on the basis of the provisions of the Treaties relating to these areas shall not entail harmonisation of Member States’ laws or regulations.

6. The scope of and arrangements for exercising the Union’s competences shall be determined by the provisions of the Treaties relating to each area.

Article 3

1. The Union shall have exclusive competence in the following areas:
   (a) customs union;
   (b) the establishing of the competition rules necessary for the functioning of the internal market;
   (c) monetary policy for the Member States whose currency is the euro;
   (d) the conservation of marine biological resources under the common fisheries policy;
   (e) common commercial policy.

2. The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.

Article 4

1. The Union shall share competence with the Member States where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6.

2. Shared competence between the Union and the Member States applies in the following principal areas:
   (a) internal market;
   (b) social policy, for the aspects defined in this Treaty;
   (c) economic, social and territorial cohesion;
   (d) agriculture and fisheries, excluding the conservation of marine biological resources;
   (e) environment;
   (f) consumer protection;
   (g) transport;
   (h) trans-European networks;
   (i) energy;
   (j) area of freedom, security and justice;
   (k) common safety concerns in public health matters, for the aspects defined in this Treaty.

3. In the areas of research, technological development and space, the Union shall have competence to carry out activities, in particular to define and implement programmes; however, the exercise of that competence shall not result in Member States being prevented from exercising theirs.

4. In the areas of development cooperation and humanitarian aid, the Union shall have competence to carry out activities and conduct a common policy; however, the exercise of that competence shall not result in Member States being prevented from exercising theirs.

Article 5
1. The Member States shall coordinate their economic policies within the Union. To this end, the Council shall adopt measures, in particular broad guidelines for these policies. Specific provisions shall apply to those Member States whose currency is the euro.

2. The Union shall take measures to ensure coordination of the employment policies of the Member States, in particular by defining guidelines for these policies.

3. The Union may take initiatives to ensure coordination of Member States' social policies.

**Article 6**

The Union shall have competence to carry out actions to support, coordinate or supplement the actions of the Member States. The areas of such action shall, at European level, be:

(a) protection and improvement of human health;
(b) industry;
(c) culture;
(d) tourism;
(e) education, vocational training, youth and sport;
(f) civil protection;
(g) administrative cooperation.

**TITLE II**

**PROVISIONS HAVING GENERAL APPLICATION**

**Article 7**

The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.

**Article 8**

In all its activities, the Union shall aim to eliminate inequalities, and to promote equality, between men and women.

**Article 9**

In defining and implementing its policies and activities, the Union shall take into account requirements linked to the promotion of a high level of employment, the guarantee of adequate social protection, the fight against social exclusion, and a high level of education, training and protection of human health.

**Article 10**

In defining and implementing its policies and activities, the Union shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

**Article 11**

Environmental protection requirements must be integrated into the definition and implementation of the Union’s policies and activities, in particular with a view to promoting sustainable development.

**Article 12**

Consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities.

**Article 13**

In formulating and implementing the Union’s agriculture, fisheries, transport, internal market, research and technological development and space policies, the Union and the Member States shall, since animals are sentient beings, pay full regard to the welfare requirements of animals, while respecting the legislative or administrative provisions and customs of the Member States relating in particular to religious rites, cultural traditions and regional heritage.

**Article 14**

Without prejudice to Article 4 of the Treaty on European Union or to Articles 93, 106 and 107 of this Treaty, and given the place occupied by services of general economic interest in the shared values of the Union as well as their role in promoting social and territorial cohesion, the Union and the Member States, each within their respective powers and within the scope of application of the Treaties, shall take care that such services operate on the basis of principles and conditions, particularly economic and financial conditions, which enable them to fulfill their missions. The European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall establish these principles and set these conditions without prejudice to the competence of Member States, in compliance with the Treaties, to provide, to commission and to fund such services.

**Article 15**

1. In order to promote good governance and ensure the participation of civil society, the Union’s institutions, bodies, offices and agencies shall conduct their work as openly as possible.

2. The European Parliament shall meet in public, as shall the Council when considering and voting on a draft legislative act.

3. Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union’s institutions, bodies, offices and agencies, whatever their medium, subject to the principles and the conditions to be defined in accordance with this paragraph.

General principles and limits on grounds of public or private interest governing this right of access to documents shall be determined by the European Parliament and the Council, by means of regulations, acting in accordance with the ordinary legislative procedure.

Each institution, body, office or agency shall ensure that its proceedings are transparent and shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents, in accordance with the regulations referred to in the second subparagraph.

The Court of Justice of the European Union, the European Central Bank and the European Investment Bank shall be subject to this paragraph only when exercising their administrative tasks.

The European Parliament and the Council shall ensure publication of the documents relating to the legislative procedures under the terms laid down by the regulations referred to in the second subparagraph.

**Article 16**

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

**Article 17**

1. The Union respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States.

2. The Union equally respects the status under national law of philosophical and non-confessional organisations.
3. Recognising their identity and their specific contribution, the Union shall maintain an open, transparent and regular dialogue with these churches and organisations.

PART THREE - TITLE II FREE MOVEMENT OF GOODS

Article 28
1. The Union shall comprise a customs union which shall cover all trade in goods and which shall involve the prohibition between Member States of customs duties on imports and exports and of all charges having equivalent effect, and the adoption of a common customs tariff in their relations with third countries, in Member States and to products coming from third countries which are in free circulation in Member States.

Article 29
Products coming from a third country shall be considered to be in free circulation in a Member State if the import formalities have been complied with and any customs duties or charges having equivalent effect which are payable have been levied in that Member State, and if they have not benefited from a total or partial drawback of such duties or charges.

CHAPTER 1
THE CUSTOMS UNION

Article 30
Customs duties on imports and exports and charges having equivalent effect shall be prohibited between Member States. This prohibition shall also apply to customs duties of a fiscal nature.

Article 31
Common Customs Tariff duties shall be fixed by the Council on a proposal from the Commission.

Article 32
In carrying out the tasks entrusted to it under this Chapter the Commission shall be guided by:
(a) the need to promote trade between Member States and third countries;
(b) developments in conditions of competition within the Union in so far as they lead to an improvement in the competitive capacity of undertakings;
(c) the requirements of the Union as regards the supply of raw materials and semi-finished goods; in this connection the Commission shall take care to avoid distorting conditions of competition between Member States in respect of finished goods;
(d) the need to avoid serious disturbances in the economies of Member States and to ensure national development of production and an expansion of consumption within the Union.

CHAPTER 2
CUSTOMS COOPERATION

Article 33
Within the scope of application of the Treaties, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall take measures in order to strengthen customs cooperation between Member States and between the latter and the Commission.

CHAPTER 3
PROHIBITION OF QUANTITATIVE RESTRICTIONS BETWEEN MEMBER STATES

Article 34
Quantitative restrictions on imports and all measures having equivalent effect shall be prohibited between Member States.

Article 35
Quantitative restrictions on exports, and all measures having equivalent effect, shall be prohibited between Member States.

Article 36
The provisions of Articles 34 and 35 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States.

Article 37
1. Member States shall adjust any State monopolies of a commercial character so as to ensure that no discrimination regarding the conditions under which goods are procured and marketed exists between nationals of Member States. In fact, either directly or indirectly supervises, determines or appreciably influences imports or exports between Member States. These provisions shall likewise apply to monopolies delegated by the State to others.
2. Member States shall refrain from introducing any new measure which is contrary to the principles laid down in paragraph 1 or which restricts the scope of the articles dealing with the prohibition of customs duties and quantitative restrictions between Member States.
3. If a State monopoly of a commercial character has rules which are designed to make it easier to dispose of agricultural products or obtain for them the best return, steps should be taken in applying the rules contained in this Article to ensure equivalent safeguards for the employment and standard of living of the producers concerned.

PART THREE - TITLE IV FREE MOVEMENT OF PERSONS, SERVICES AND CAPITAL

CHAPTER 2
RIGHT OF ESTABLISHMENT

Article 49
Within the framework of the provisions set out below, restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State shall be prohibited. Such prohibition shall also apply to restrictions on the setting-up of agencies, branches or subsidiaries by nationals of any Member State established in the territory of any Member State.
Freedom of establishment shall include the right to take up and pursue activities as self-employed persons and to set up and manage undertakings, in particular companies or firms within the meaning of the second paragraph of Article 54, under the conditions laid down for its own nationals by the law of the country where such establishment is effected, subject to the provisions of the Chapter relating to capital.

Article 50
1. In order to attain freedom of establishment as regards a particular activity, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, shall act by means of directive.
2. The European Parliament, the Council and the Commission shall carry out the duties devolving upon them under the preceding provisions, in particular:
(a) by agreeing, as a general rule, priority treatment to activities where freedom of establishment makes a particularly valuable contribution to the development of production and trade;
(b) by ensuring close cooperation between the competent authorities in the Member States in order to ascertain the
particular situation within the Union of the various activities concerned;
(c) by abolishing those administrative procedures and practices, whether resulting from national legislation or from agreements previously concluded between Member States, the maintenance of which would form an obstacle to freedom of establishment;
(d) by ensuring that workers of one Member State employed in the territory of another Member State may remain in that territory for the purpose of taking up activities therein as self-employed persons, where they satisfy the conditions which they would be required to satisfy if they were entering that State at the time when they intended to take up such activities;
(e) by enabling a national of one Member State to acquire and use land and buildings situated in the territory of another Member State, in so far as this does not conflict with the principles laid down in Article 39(2);
(f) by effecting the progressive abolition of restrictions on freedom of establishment in every branch of activity under consideration, both as regards the conditions for setting up agencies, branches or subsidiaries in the territory of a Member State and as regards the subsidiaries in the territory of a Member State and as regards the conditions governing the entry of personnel belonging to the main establishment into managerial or supervisory posts in such agencies, branches or subsidiaries;
(g) by coordinating to the necessary extent the safeguards which, for the protection of the interests of members and others, are required by Member States of companies or firms within the meaning of the second paragraph of Article 54 with a view to making such safeguards equivalent throughout the Union;
(h) by satisfying themselves that the conditions of establishment are not distorted by aids granted by Member States.

Article 51
The provisions of this Chapter shall not apply, so far as any given Member State is concerned, to activities which in that State are connected, even occasionally, with the exercise of official authority. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may rule that the provisions of this Chapter shall not apply to certain activities.

Article 52
1. The provisions of this Chapter and measures taken in pursuance thereof shall not prejudice the applicability of provisions laid down by law, regulation or administrative action providing for special treatment for foreign nationals on grounds of public policy, public security or public health.
2. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure, issue directives for the coordination of the abovementioned provisions.

Article 53
1. In order to make it easier for persons to take up and pursue activities as self-employed persons, the European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure, issue directives for the mutual recognition of diplomas, certificates and other evidence of formal qualifications and for the coordination of the provisions laid down by law, regulation or administrative action in Member States concerning the taking-up and pursuit of activities as self-employed persons.
2. In the case of the medical and allied and pharmaceutical professions, the progressive abolition of restrictions shall be dependent upon coordination of the conditions for their exercise in the various Member States.

Article 54
Companies or firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Union shall, for the purposes of this Chapter, be treated in the same way as natural persons who are nationals of Member States. ‘Companies or firms’ means companies or firms constituted under civil or commercial law, including cooperative societies, and other legal persons governed by public or private law, save for those which are non-profit-making.

Article 55
Member States shall accord nationals of the other Member States the same treatment as their own nationals as regards participation in the capital of companies or firms within the meaning of Article 54, without prejudice to the application of the other provisions of the Treaties.

CHAPTER 3 SERVICES

Article 56
Within the framework of the provisions set out below, restrictions on freedom to provide services within the Union shall be prohibited in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may extend the provisions of the Chapter to nationals of a third country who provide services and who are established within the Union.

Article 57
Services shall be considered to be ‘services’ within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons.

Services’ shall in particular include:
(a) activities of an industrial character;
(b) activities of a commercial character;
(c) activities of craftsmen;
(d) activities of the professions.
Without prejudice to the provisions of the Chapter relating to the right of establishment, the person providing a service may, in order to do so, temporarily pursue his activity in the Member State where the service is provided, under the same conditions as are imposed by that State on its own nationals.

Article 58
1. Freedom to provide services in the field of transport shall be governed by the provisions of the Title relating to transport.
2. The liberalisation of banking and insurance services connected with movements of capital shall be effected in step with the liberalisation of movement of capital.

Article 59
1. In order to achieve the liberalisation of a specific service, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, shall issue directives.
2. As regards the directives referred to in paragraph 1, priority shall as a general rule be given to those services which directly affect production costs or the liberalisation of which helps to promote trade in goods.

Article 60
The Member States shall endeavour to undertake the liberalisation of services beyond the extent required by the directives issued pursuant to Article 59(1), if their general economic situation and the situation of the economic sector concerned so permit.
To this end, the Commission shall make recommendations to the Member States concerned.

Article 61
As long as restrictions on freedom to provide services have not been abolished, each Member State shall apply such restrictions without distinction on grounds of nationality or residence to all persons providing services within the meaning of the first paragraph of Article 56.

**Article 62**
The provisions of Articles 51 to 54 shall apply to the matters covered by this Chapter.

**TITLE XV CONSUMER PROTECTION**

**Article 169**

1. In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests.

2. The Union shall contribute to the attainment of the objectives referred to in paragraph 1 through:

(a) measures adopted pursuant to Article 114 in the context of the completion of the internal market;

(b) measures which support, supplement and monitor the policy pursued by the Member States.

3. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, shall adopt the measures referred to in paragraph 2(b).

4. Measures adopted pursuant to paragraph 3 shall not prevent any Member State from maintaining or introducing more stringent protective measures. Such measures must be compatible with the Treaties. The Commission shall be notified of them.

**Relevant Case-Law on free movement of goods and services (on-line)**

*Case C-322/01, Deutscher Apothekerverband eV and 0800 DocMorris NV,*

**Summary of the Judgment**

1. **Free movement of goods – Quantitative restrictions – Measures having equivalent effect – Definition – Prohibition on the sale by mail order of medicinal products the sale of which is restricted to pharmacies – Whether included – Justification limited to medicinal products subject to prescription – Reimportation of medicinal products into the Member State concerned – Not relevant**

* (Arts 28 EC and 30 EC)

2. **Approximation of laws – Proprietary medicinal products – Advertising – Prohibition on advertising the sale by mail order of medicinal products the sale of which is restricted to pharmacies – Permissible only in respect of medicinal products subject to prescription**


1. Commercial rules which govern the arrangements for the sale of products constitute measures of equivalent effect for the purposes of Article 28 EC if they do not apply to all relevant traders operating in national territory and if they do not affect in the same manner, in law and in fact, the marketing of both domestic products and those from other Member States. A national prohibition on the sale by mail order of medicinal products the sale of which is restricted to pharmacies in the Member State concerned is in that regard a measure having an effect equivalent to a quantitative restriction where the prohibition has a greater impact on pharmacies established outside the national territory and could impede access to the market for products from other Member States more than it impedes access for domestic products. Article 30 EC may, however, be relied on to justify such a national prohibition on the sale by mail order of medicinal products in so far as the prohibition covers medicinal products subject to prescription. Given that there may be risks attaching to the use of these medicinal products, the need to be able to check effectively and responsibly the authenticity of doctors' prescriptions and to ensure that the medicine is handed over either to the customer himself, or to a person to whom its collection has been entrusted by the customer, is such as to justify a prohibition on mail-order sales. However, Article 30 EC cannot be relied on to justify an absolute prohibition on the sale by mail order of medicinal products which are not subject to prescription in the Member State concerned. Those findings do not need to be assessed differently where medicinal products are imported into a Member State in which they are authorised, having been previously obtained by a pharmacy in another Member State from a wholesaler in the importing Member State. see paras 68, 74, 76, 112, 119, 124, 134, operative part 1

2. Article 88(1) of Directive 2001/83 on the Community code relating to medicinal products for human use, which prohibits advertising for prescription medicines, precludes a national prohibition on advertising the sale by mail order of medicinal products which may be supplied only in pharmacies in the Member State concerned in so far as the prohibition covers medicinal products which are not subject to prescription. Article 88(2) of the Community Code, which allows medicinal products not subject to prescription to be advertised to the general public, cannot be interpreted as precluding advertising for the sale by mail order of medicines on the basis of the alleged need for a pharmacist to be physically present, since the prohibition on the sale by mail order cannot itself be justified, in relation to non-prescription medicines, by that alleged need. see pans 143-144, 148, operative part 2

THE COURT, in answer to the questions referred to it by the Landgericht Frankfurt am Main by order of 10 August 2001, hereby rules:

1. (a) A national prohibition on the sale by mail order of medicinal products the sale of which is restricted to pharmacies in the Member State concerned, such as the prohibition laid down in Paragraph 43(1) of the Arzneimittelgesetz (Law on medicinal products) in the version of 7 September 1998, is a measure having an effect equivalent to a quantitative restriction for the purposes of Article 28 EC.

(b) Article 30 EC may be relied on to justify a national prohibition on the sale by mail order of medicinal products which may be sold only in pharmacies in the Member State
concerned in so far as the prohibition covers medicinal products subject to prescription. However, Article 30 EC cannot be relied on to justify an absolute prohibition on the sale by mail order of medicinal products which are not subject to prescription in the Member State concerned.

(c) Questions 1(a) and 1(b) do not need to be assessed differently where medicinal products are imported into a Member State in which they are authorised, having been previously obtained by a pharmacy in another Member State from a wholesaler in the importing Member State.

2. Article 88(1) of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use precludes a national prohibition on advertising the sale by mail order of medicinal products which may be supplied only in pharmacies in the Member State concerned, such as the prohibition laid down in Paragraph 8(1) of the Heilmittelvergebungsgesetz (Law on the advertising of medicinal products), in so far as the prohibition covers medicinal products which are not subject to prescription.

**Case C-243/01 Criminal proceedings against Piergiorgio Gambelli and Others**

**Ruling**

National legislation which prohibits on pain of criminal penalties the pursuit of the activities of collecting, taking, booking and forwarding offers of bets, in particular bets on sporting events, without a licence or authorisation from the Member State concerned constitutes a restriction on the freedom of establishment and the freedom to provide services provided for in Articles 43 and 49 EC respectively. It is for the national court to determine whether such legislation, taking account of the detailed rules for its application, actually serves the aims which might justify it, and whether the restrictions it imposes are disproportionate in the light of those objectives.

**Case C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International Ltd, formerly Baw International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa**

**Summary of the Judgment**

1. Freedom to provide services – Provisions of the Treaty – Scope (Arts 49 EC and 56 EC)
2. Freedom to provide services – Restrictions (Art. 49 EC)

1. Any restrictive effects which the legislation of a Member State, which prohibits operators established in other Member States in which they lawfully provide similar services from offering games of chance via the internet within the territory of that Member State, might have on the free movement of capital and payments would be no more than the inevitable consequence of any restrictions on the freedom to provide services. Where a national measure relates to several fundamental freedoms at the same time, the Court will in principle examine the measure in relation to only one of those freedoms if it appears, in the circumstances of the case, that the other freedoms are entirely secondary in relation to the first and may be considered together with it. (see para. 47)

2. Article 49 EC does not preclude legislation of a Member State which prohibits private operators established in other Member States, in which they lawfully provide similar services, from offering games of chance via the internet within the territory of that Member State.

Admittedly, such legislation gives rise to a restriction of the freedom to provide services enshrined in Article 49 EC, by also imposing a restriction on the freedom of the residents of the Member State concerned to enjoy, via the internet, services which are offered in other Member States.

However, in the light of the specific features associated with the provision of games of chance via the internet, the restriction at issue may be regarded as justified by the objective of combating fraud and crime. The grant of exclusive rights to operate games of chance via the internet to a single operator which is subject to strict control by the public authorities may confine the operation of gambling within controlled channels and be regarded as appropriate for the purpose of protecting consumers against fraud on the part of operators.

As to whether the system in dispute is necessary, the sector involving games of chance offered via the internet has not been the subject of Community harmonisation. A Member State is therefore entitled to take the view that the mere fact that a private operator lawfully offers services in that sector via the internet in another Member State, in which it is established and where it is in principle already subject to statutory conditions and controls on the part of the competent authorities in that State, cannot be regarded as amounting to a sufficient assurance that national consumers will be protected against the risks of fraud and crime, in the light of the difficulties liable to be encountered in such a context by the authorities of the Member State of establishment in assessing the professional qualities and integrity of operators. In addition, because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators against consumers compared with the traditional markets for such games. Moreover, the possibility cannot be ruled out that an operator which sponsors some of the sporting competitions on which it accepts bets and some of the teams taking part in those competitions may be in a position to influence their outcome directly or indirectly, and thus increase its profits. (see paras 53-54, 67-73, operative part).

1. This request for a preliminary ruling concerns the interpretation of Article 56 EC.

18. In those circumstances, the Bundesgerichtshof decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

‘1. Does it represent an inconsistent restriction on gaming and betting activities where, on the one hand, in a Member State organised as a federal State, the organisation and facilitation of public games of chance on the internet is, in principle, prohibited by the law in force in the overwhelming majority of the Länder and — without an established right — can be allowed, exceptionally, only for lotteries and sporting bets in order to provide a suitable alternative to the illegal supply of games of chance as well as to combat the development and spread thereof, but — on the other hand, under the law in force in one of that Member State’s Länder, subject to certain specified objective conditions, an authorisation for the marketing of sporting bets on the internet must be issued to any EU citizen or equivalent legal person, thereby undermining the effectiveness of the restriction on the marketing of games of chance on the internet in force in the rest of the Federal Republic in achieving the legitimate public interest objectives which it pursues?’

2. Does the answer to the first question depend on whether the different legal position in one Land removes altogether or significantly undermines the effectiveness of the restrictions
on the marketing of games of chance on the internet in force in the other Länder in achieving the legitimate public interest objectives which they pursue?

If the answer to the first question is in the affirmative:

3. Is the inconsistency avoided by the Land with the divergent legislation adopting the restrictions on games of chance in force in the rest of the Länder, even where, in relation to the administrative licensing contracts already concluded there, the previous more generous rules on internet games of chance in that Land remain in force for a transitional period of several years because those authorisations cannot be revoked, or cannot be revoked without incurring compensation payments which the Land would find difficult to bear?

4. Does the answer to the third question depend on whether, during the transition period of several years, the effectiveness of the restrictions on games of chance in force in the other Länder is affected or significantly undermined?

Ruling: Article 56 TFEU must be interpreted as meaning that it does not preclude legislation common to the majority of the federal entities of a Member State having a federal structure which prohibits, in principle, the organisation and facilitation of games of chance via the internet, where, for a limited period, a single federal entity has maintained in force more liberal legislation coexisting with the restrictive legislation of the other federal entities, provided that such legislation is able to satisfy the conditions of proportionality laid down by the case-law of the Court, which is for the national court to ascertain.


(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
Having regard to the opinion of the European Economic and Social Committee (1),
Having regard to the opinion of the Committee of the Regions (2),
Acting in accordance with the ordinary legislative procedure (3),

Whereas:


(2) Those Directives have been reviewed in the light of experience with a view to simplifying and updating the applicable rules, removing inconsistencies and closing unwanted gaps in the rules. That review has shown that it is appropriate to replace those two Directives by a single Directive. This Directive should therefore lay down standard rules for the common aspects of distance and off-premises contracts, moving away from the minimum harmonisation approach in the former Directives whilst allowing Member States to maintain or adopt national rules in relation to certain aspects.

(3) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through the measures adopted pursuant to Article 114 thereof.

(4) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured. The harmonisation of certain aspects of consumer distance and off-premises contracts is necessary for the promotion of a real consumer internal market striking the right balance between a high level of consumer protection and the competitiveness of enterprises, while ensuring respect for the principle of subsidiarity.

(5) The cross-border potential of distance selling, which should be one of the main tangible results of the internal market, is not fully exploited. Compared with the growth of domestic trade in the last few years, the growth in cross-border distance sales has been limited. This discrepancy is particularly significant for Internet sales for which the potential for further growth is high. The cross-border potential of contracts negotiated away from business premises (direct selling) is constrained by a number of factors including the different national consumer protection rules imposed upon the industry. Compared with the growth of domestic direct selling over the last few years, in particular in the services sector, for instance utilities, the number of consumers using this channel for cross-border purchases has remained flat. Responding to increased business opportunities in many Member States, small and medium-sized enterprises (including individual traders) or agents of direct selling companies should be more inclined to seek business opportunities in other Member States, in particular in border regions. Therefore the full harmonisation of consumer information and the right of withdrawal in distance and off-premises contracts will contribute to a high level of consumer protection and a better functioning of the business-to-consumer internal market.

(6) Certain disparities create significant internal market barriers affecting traders and consumers. Those disparities increase compliance costs to traders wishing to engage in the cross-border sale of goods or provision of services. Disproportionate fragmentation also undermines consumer confidence in the internal market.

(7) Full harmonisation of some key regulatory aspects should considerably increase legal certainty for both consumers and traders. Both consumers and traders should be able to rely on a single regulatory framework based on clearly defined legal concepts regulating certain aspects of business-to-consumer contracts across the Union. The effect of such harmonisation should be to eliminate the barriers stemming from the fragmentation of the rules and to complete the internal market in this area. Those barriers can only be eliminated by establishing uniform rules at Union
level. Furthermore consumers should enjoy a high common level of protection across the Union.

(8) The regulatory aspects to be harmonised should only concern contracts concluded between traders and consumers. Therefore, this Directive should not affect national law in the area of contracts relating to sale and supply agreements, contracts relating to succession rights, contracts relating to family law and contracts relating to the incorporation and organisation of companies or partnership agreements.

(9) This Directive establishes rules on information to be provided for distance contracts, off-premises contracts and contracts other than distance and off-premises contracts. This Directive also regulates the right of withdrawal for distance and off-premises contracts and harmonises certain provisions dealing with the performance and some other aspects of business-to-consumer contracts.

(10) This Directive should be without prejudice to contractual obligations (Rome I) (6).

(11) This Directive should be without prejudice to Union provisions relating to specific sectors, such as medicinal products for human use, medical devices, privacy and electronic communications, patients’ rights in cross-border healthcare, food labelling and the internal market for electricity and natural gas.

(12) The information requirements provided for in this Directive should not be considered a distance contract. By contrast, a contract concludes the contract at a distance. By contrast, a contract concludes the contract at a distance. That definition should also cover situations where the consumer visits the business premises for purposes partly within the scope of this Directive, for example because they are not concluded under an organised distance sales or service provision scheme. Member States may therefore maintain or introduce national legislation corresponding to the provisions of this Directive, or certain of its provisions, in relation to contracts that fall outside the scope of this Directive. For instance, Member States may decide to extend the application of the rules of this Directive to legal persons or to natural persons who are not consumers within the meaning of this Directive, such as non-governmental organisations, start-ups or small and medium-sized enterprises. Similarly, Member States may apply the provisions of this Directive to contracts that are not distance contracts within the meaning of this Directive, for example for instance for the tracking of consumer behaviour; it should also refer to the absence or presence of any technical restrictions such as protection via Digital Rights Management or region coding. The notion of relevant interoperability of digital content is meant to describe the information and technology involved with which the digital content is compatible, for instance the operating system, the necessary version and certain hardware features. The Commission should examine the need for further harmonisation of provisions in respect of digital content and submit, if necessary, a legislative proposal for addressing this matter.

(20) The definition of distance contract should cover all cases where a contract is concluded between the trader and the consumer under an organised distance sales or service provision scheme, with the exclusive use of one or more means of distance communication (such as mail order, Internet, telephone or mobile phone) and including the time at which the contract is concluded. That definition should also cover situations where the consumer visits the business premises merely for the purpose of gathering information about the goods or services and subsequently negotiates and concludes the contract at a distance. By contrast, a contract which is negotiated at the business premises of the trader and finally concluded by means of distance communication should not be considered a distance contract. Neither should a contract initiated by means of distance communication, but finally concluded at the business premises of the trader be considered a distance contract. Similarly, the concept of distance contract should not include reservations made by a...
the consumer and hired and hire buildings as well as contracts for the trader. Market premises and/or services and his interests stemming from his relationship with the trader. (23) Durable media should enable the consumer to store the meaning of this Directive.

The business premises of a person acting in the exceptional basis for his business activities as well as private homes or workplaces should not be regarded as business premises context but the contract is concluded with the simultaneous physical presence of the consumer, the total cost thereof should be taken into account at a sufficiently low level as to exclude only purchases of Directive where goods or services of a minor value are sold off-premises. The monetary threshold should be established at a sufficiently low level as to exclude only purchases of small significance. Member States should be allowed to define this value in their national legislation provided that it does not exceed EUR 50. Where two or more contracts with related subjects are concluded at the same time by the consumer, the total cost thereof should be taken into account for the purpose of applying this threshold.

(24) A contract for the supply of heat, inter alia, in the form of steam or hot water, from a central source of production through a transmission and distribution system to multiple buildings, for the purpose of heating.

(25) Contracts related to the transfer of immovable property or of rights in immovable property or to the creation or acquisition of such immovable property or rights, contracts for the construction of new buildings or the substantial conversion of existing buildings as well as contracts for the rental of accommodation for residential purposes are already subject to a number of specific requirements in national legislation. Those contracts include for instance sales of immovable property still to be developed and hire-purchase. The provisions of this Directive are not appropriate to those contracts, which should be therefore excluded from its scope. A substantial conversion is a conversion comparable to the construction of a new building, for example where only the façade of an old building is retained. Service contracts in particular those related to the construction of annexes to buildings (for example a garage or a veranda) and those related to repair and renovation of buildings other than substantial conversion, should be included in the scope of this Directive, as well as contracts related to the services of a real estate agent and those related to the rental of accommodation for non-residential purposes.

(26) Contracts related to the transfer of immovable property or of rights in immovable property or to the creation or acquisition of such immovable property or rights, contracts for the construction of new buildings or the substantial conversion of existing buildings as well as contracts for the rental of accommodation for residential purposes are already subject to a number of specific requirements in national legislation. Those contracts include for instance sales of immovable property still to be developed and hire-purchase. The provisions of this Directive are not appropriate to those contracts, which should be therefore excluded from its scope. A substantial conversion is a conversion comparable to the construction of a new building, for example where only the façade of an old building is retained. Service contracts in particular those related to the construction of annexes to buildings (for example a garage or a veranda) and those related to repair and renovation of buildings other than substantial conversion, should be included in the scope of this Directive, as well as contracts related to the services of a real estate agent and those related to the rental of accommodation for non-residential purposes.

(27) Transport services cover passenger transport and transport of goods. Passenger transport should be excluded from the scope of this Directive as it is subject to other Union legislation or, in the case of public transport and taxis, to regulation at national level. However, the provisions of this Directive protecting consumers against excessive fees for the use of means of payment or against hidden costs should apply also to passenger transport contracts. In relation to transport of goods and car rental which are services, consumers should benefit from the protection afforded by this Directive, with the exception of the right of withdrawal.

(28) In order to avoid administrative burden being placed on traders, Member States may decide not to apply this Directive where goods or services of a minor value are sold off-premises. The monetary threshold should be established at a sufficiently low level as to exclude only purchases of small significance. Member States should be allowed to define this value in their national legislation provided that it does not exceed EUR 50. Where two or more contracts with related subjects are concluded at the same time by the consumer, the total cost thereof should be taken into account for the purpose of applying this threshold.

(29) Social services have fundamentally distinct features that are reflected in sector-specific legislation, partially at Union level and partially in national law. Social services include on the one hand, services for particularly disadvantaged or low income persons as well as services for persons and families in need of assistance in carrying out routine, everyday tasks and, on the other hand, services for all people who have a special need for assistance, support, protection or encouragement in a specific life phase. Social services cover, inter alia, services for children and youth, assistance services for families, single parents or older persons, and services for migrants. Social services cover both short-term and long-term care services, for instance services provided by home care services or other living facilities and residential homes or housing (‘nursing homes’). Social services include not only those provided by the State at a national, regional or local level by providers mandated by the State or by charities recognised by the State but also those provided by private operators. The provisions of this Directive are not appropriate to social services which should be therefore excluded from its scope.

(30) Healthcare requires special regulations because of its technical complexity, its importance as a service of general interest as well as its extensive public funding. Healthcare is defined in Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of...
patients’ rights in cross-border healthcare (9) as ‘health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices’. Health professional is defined in that Directive as a doctor of medicine, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (10) or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in point (a) of Article 3(1) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment. The provisions of this Directive are not appropriate to healthcare which should be therefore excluded from its scope.

(31) Gambling should be excluded from the scope of this Directive. Gambling activities are those which involve wagering at stake with pecuniary value in games of chance, including lotteries, gambling in casinos and betting transactions. Member States should be able to adopt other, including more stringent, consumer protection measures in relation to such activities.

(32) The existing Union legislation, inter alia, relating to consumer financial services, package travel and timeshare contains numerous rules on consumer protection. For this reason, this Directive should not apply to contracts in those areas. With regard to financial services, Member States should be encouraged to draw inspiration from existing Union legislation in that area when legislating in areas not regulated at Union level, in such a way that a level playing field for all consumers and all contracts relating to financial services is ensured.

(33) The trader should be obliged to inform the consumer in advance of any arrangement resulting in the consumer paying a deposit to the trader, including an arrangement whereby an amount is blocked on the consumer’s credit or debit card.

(34) The trader should give the consumer clear and comprehensible information before the consumer is bound by a distance or off-premises contract, a contract other than a distance or an off-premises contract, or any corresponding offer. In providing that information, the trader should take into account the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee. However, taking into account such specific needs should not lead to different levels of consumer protection.

(35) The information to be provided by the trader to the consumer should be mandatory and should not be altered. Nevertheless, the contracting parties should be able to expressly agree to change the content of the contract subsequently concluded, for instance the arrangements for delivery.

(36) In the case of distance contracts, the information requirements should be adapted to take into account the technical constraints of certain media, such as the restrictions on the number of characters on certain mobile telephone screens or the time constraint on television sales spots. In such cases the trader should comply with a minimum set of information requirements and refer the consumer to another source of information, for instance by providing a toll free telephone number or a hypertext link to a webpage of the trader where the relevant information is directly available and easily accessible. As to the requirement to inform the consumer of the costs of returning goods which by their nature cannot normally be returned by post, it will be considered to have been met, for example, if the trader specifies one carrier (for instance the one he assigned for the delivery of the good) and one price concerning the cost of returning the goods. Where the cost of returning the goods cannot reasonably be calculated in advance by the trader, for example because the trader does not offer to arrange for the return of the goods himself, the trader should provide a statement that such a cost will be payable, and that this cost may be high, along with a reasonable estimation of the maximum cost, which could be based on the cost of delivery to the consumer.

(37) Since in the case of distance sales, the consumer is not able to see the goods before concluding the contract, he should have a right of withdrawal. For the same reason, the consumer should be allowed to test and inspect the goods he has bought to the extent necessary to establish the nature, characteristics and the functioning of the goods. Concerning off-premises contracts, the consumer should have the right of withdrawal because of the potential surprise element and/or psychological pressure. Withdrawal from the contract should terminate the obligation of the contracting parties to perform the contract.

(38) Trading websites should indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

(39) It is important to ensure for distance contracts concluded through websites that the consumer is able to fully read and understand the main elements of the contract before placing his order. To that end, provision should be made in this Directive for those elements to be displayed in the close vicinity of the confirmation requested for placing the order. It is also important to ensure that, in such situations, the consumer is able to determine the moment at which he assumes the obligation to pay the trader. Therefore, the consumer’s attention should specifically be drawn, through an unambiguous formulation, to the fact that placing the order entails the obligation to pay the trader.

(40) The current varying lengths of the withdrawal periods both between the Member States and for distance and off-premises contracts cause legal uncertainty and compliance costs. The same withdrawal period should apply to all distance and off-premises contracts. In the case of service contracts, the withdrawal period should expire after 14 days from the conclusion of the contract. In the case of sales contracts, the withdrawal period should expire after 14 days from the day on which the consumer or a third party other than the carrier and indicated by the consumer, acquires physical possession of the goods. In addition the consumer should be able to exercise the right to withdraw before acquiring physical possession of the goods. Where multiple goods are ordered by the consumer in one order but are delivered separately, the withdrawal period should expire after 14 days from the day on which the consumer acquires physical possession of the last good. Where goods are delivered in multiple lots or pieces, the withdrawal period should expire after 14 days from the day on which the consumer acquires the physical possession of the last lot or piece.

(41) In order to ensure legal certainty, it is appropriate that Council Regulation (EC) Euratom No 1102/71 of 3 June 1971 determining the rules applicable to periods, dates and time limits (11) should apply to the calculation of the periods contained in this Directive. Therefore, all periods contained in this Directive should be considered as falling within the period in question.

(42) The provisions relating to the right of withdrawal should be without prejudice to the Member States’ laws and regulations governing the cost of delivery and/or the termination or unenforceability of a contract or the possibility for the consumer to fulfill his contractual obligations before the time determined in the contract.

(43) If the trader has not adequately informed the consumer prior to the conclusion of a distance or off-premises contract, the withdrawal period should be extended. However, in
order to ensure legal certainty as regards the length of the withdrawal period, a 12-month limitation period should be introduced.

(44) Differences in the ways in which the right of withdrawal is exercised in the Member States have caused costs for traders selling cross-border. The introduction of a harmonised model withdrawal form that the consumer may use should simplify the withdrawal process and bring legal certainty. For these reasons, Member States should refrain from adding any presentational requirements to the Union-wide model form relating for example to the font size. However, the consumer should remain free to withdraw in his own words, provided that his statement setting out his decision to withdraw from the contract to the trader is unequivocal. A letter, a telephone call or returning the goods with a clear statement could meet this requirement, but the burden of proving having withdrawn within the time limits fixed in the Directive should be on the consumer. For this reason, it is in the interest of the consumer to make use of a durable medium when communicating his withdrawal to the trader.

(45) As experience shows that many consumers and traders prefer to communicate via the trader’s website, there should be a possibility for the trader to give the consumer the option of filing in a web-based withdrawal form. In this case the trader should provide an acknowledgement of receipt for instance by e-mail without delay.

(46) If the consumer withdraws from the contract, the trader should reimburse all payments received from the consumer, including those covering the expenses borne by the trader to deliver goods to the consumer. The reimbursement should not be made by voucher unless the consumer has used vouchers for the initial transaction or has expressly accepted them. If the consumer expressly chooses a certain type of delivery (for instance 24-hour express delivery), although the trader had offered a common and generally acceptable type of delivery which would have incurred lower delivery costs, the consumer should bear the difference in costs between these two types of delivery.

(47) Some consumers exercise their right of withdrawal after having used the goods to an extent more than necessary to establish the nature, characteristics and functioning of the goods. In this case the consumer should not lose the right to withdraw but should be liable for any diminished value of the goods. In order to establish the nature, characteristics and functioning of the goods, the consumer should only handle and inspect them in the same manner as he would be allowed to do in a shop. For example, the consumer should only try on a garment and should not be allowed to wear it. Consequently, the consumer should handle and inspect the goods with due care during the withdrawal period. The obligations of the consumer in the event of withdrawal should not discourage the consumer from exercising his right of withdrawal.

(48) The consumer should be required to send back the goods not later than 14 days after having informed the trader about his decision to withdraw from the contract. In situations where the trader or the consumer does not fulfil the obligations relating to the exercise of the right of withdrawal, penalties provided for by national legislation in accordance with this Directive should apply as well as a contract law provision.

(49) Certain exceptions from the right of withdrawal should exist, both for distance and off-premises contracts. A right of withdrawal could be inappropriate for example given the nature of particular goods or services. That is the case for example with wine supplied a long time after the conclusion of a contract of a speculative nature where the value is dependent on fluctuations in the market ("vin en primeur"). The right of withdrawal should neither apply to goods made to the consumer’s specifications or which are clearly personalised such as tailor-made curtains, nor to the supply of fuel, for example, which is a good, by nature inseparably mixed with other items after delivery. The granting of a right of withdrawal to the consumer could also be inappropriate in the case of certain services where the conclusion of the contract implies the setting aside of capacity which, if a right of withdrawal were exercised, the trader may find difficult to fill. This would for example be the case where reservations are made at hotels or concerning holiday cottages or cultural or sporting events.

(50) On the one hand, the consumer should benefit from his right of withdrawal even in case he has asked for the provision of services before the end of the withdrawal period. On the other hand, if the consumer, after the expiration of the right of withdrawal, the trader should be assured to be adequately paid for the service he has provided. The calculation of the proportionate amount should be based on the price agreed in the contract unless the consumer demonstrates that that total price is itself disproportionate, in which case the amount to be paid shall be calculated on the basis of the market value of the service provided. The market value should be defined by comparing the price of an equivalent service performed by other traders at the time of the conclusion of the contract. Therefore the consumer should request the performance of the services before the end of the withdrawal period by making this request expressly and, in the case of off-premises contracts, on a durable medium. Similarly, the trader should inform the consumer on a durable medium of any obligation to pay the proportionate costs for the services already provided. For contracts having as their object both goods and services, the provisions laid down for in this Directive on the return of goods should apply to the goods aspects and the compensation regime for services should apply to the services aspects.

(51) The main difficulties encountered by consumers and one of the main sources of disputes with traders concern durable goods. Therefore, the Directive should provide for the transfer of the ownership of the goods and the moment at which such transfer takes place, should remain subject to national law and therefore should not be affected by this Directive. The rules on delivery laid down in this Directive should include the possibility for the consumer to allow a third party to take possession of the goods either immediately or at a later date. If the parties have not agreed on a specific delivery date, the trader should deliver the goods as soon as possible, but in any event not later than 30 days from the day of the conclusion of the contract. The rules regarding late delivery should also take into account goods to be manufactured or acquired specially for the consumer which cannot be reused by the trader without considerable loss. Therefore, a rule which grants an additional reasonable period of time to the trader in certain circumstances should be provided for in this Directive. When the trader fails to deliver the goods within the period of time agreed with the consumer, before the consumer can terminate the contract, the consumer should call upon the trader to make the delivery within a reasonable additional period of time and be entitled to terminate the contract if the trader fails to deliver the goods even within that additional period of time. However, this rule should not apply if the trader has refused to deliver the goods in an unequivocal statement. Neither should it apply in circumstances where the delivery period is essential such as, for example, in the case of a wedding dress which should be delivered before the wedding. Nor should it apply in circumstances where the
consumer informs the trader that delivery on a specified date is essential. For this purpose, the consumer may use the trader’s contact details given in accordance with this Directive. In these specific cases, if the trader fails to deliver the goods on time, the consumer should be entitled to terminate the contract immediately after the expiry of the delivery period initially agreed. This Directive should be without prejudice to national provisions on the way the consumer should notify the trader of his will to terminate the contract.

(53) In addition to the consumer’s right to terminate the contract where the trader has failed to fulfill his obligations to deliver the goods in accordance with this Directive, the consumer may, in accordance with the applicable national law, have recourse to other remedies, such as granting the trader an additional period of time for delivery, enforcing the performance of the contract, withholding payment, and seeking damages.

(54) In accordance with Article 52(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (12), Member States should be able to prohibit or limit traders’ right to request charges from consumers taking into account the need to encourage competition and promote the use of efficient payment instruments. In any event, traders should be prohibited from charging consumers fees that exceed the cost borne by the trader for the use of a certain means of payment.

(55) Where the goods are dispatched by the trader to the consumer, disputes may arise, in the event of loss or damage, as to the moment at which the transfer of risk takes place. Therefore this Directive should provide that the consumer be protected against any risk of loss or damage to the goods occurring before he has acquired the physical possession of the goods. The consumer should be protected during a transport arranged or carried out by the trader, even where the consumer has chosen a particular delivery method from a range of options offered by the trader. However, that provision should not apply to contracts where it is up to the consumer to take delivery of the goods himself or to ask a carrier to take delivery. Regarding the moment of the transfer of the risk, a consumer should be considered to have acquired the physical possession of the goods when he has received them.

(56) Where organisations regarded under national law as having a legitimate interest in protecting consumer contractual rights should be afforded the right to initiate proceedings, either before a court or before an administrative authority which is competent to decide upon complaints or to initiate appropriate legal proceedings.

(57) It is necessary that Member States lay down penalties for infringements of this Directive and ensure that they are enforced. The penalties should be effective, proportionate and dissuasive.

(58) The consumer should not be deprived of the protection granted by this Directive. Where the law applicable to the contract is that of a third country, Regulation (EC) No 593/2008 should apply, in order to determine whether the consumer retains the protection granted by this Directive.

(59) The Commission, following consultation with the Member States and stakeholders, should look into the most appropriate way to ensure that all consumers are made aware of their rights at the point of sale.

(60) Since inertia selling, which consists of unsolicited supply of goods or provision of services to consumers, is prohibited by Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (“Unfair Commercial Practices Directive”) (13) but no contractual remedy is provided therein, it is necessary to introduce in this Directive the contractual remedy of exempting the consumer from the obligation to provide any consideration for such unsolicited supply or provision.


(62) It is appropriate for the Commission to review this Directive if some barriers to the internal market are identified. In its review, the Commission should pay particular attention to the possibilities granted to Member States to maintain or introduce specific national provisions including in certain areas of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (15) and Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees (16). That review could lead to a Commission proposal to amend this Directive; that proposal may include amendments to other consumer protection legislation reflecting the Commission’s Consumer Policy Strategy commitment to review the Union acquis in order to achieve a high, common level of consumer protection.

(63) Directives 93/13/EEC and 1999/44/EC should be amended to require Member States to inform the Commission about the adoption of specific national provisions in certain areas.

(64) Directives 85/577/EEC and 97/7/EC should be repealed.

(65) Since the objective of this Directive, namely, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(66) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(67) In accordance with point 34 of the Interinstitutional agreement on better law-making (17), Member States are encouraged to draw up, for themselves and in the interests of the Union, their own tables, which will, as far as possible, illustrate the correlation between this Directive and the transposition measures, and to make them public.

HAVE ADOPTED THIS DIRECTIVE.

CHAPTER I
SUBJECT MATTER, DEFINITIONS AND SCOPE

Article 1
Subject matter
The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by approximating certain aspects of the laws, regulations and administrative provisions of the Member States concerning contracts concluded between consumers and traders.

Article 2
Definitions
For the purpose of this Directive, the following definitions shall apply:
(1) ‘Consumer’ means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession;
(2) ‘Trader’ means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf for purposes relating to his trade, business,
'goods' means any tangible movable items, with the exception of items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or in a set quantity;

(4) 'goods made to the consumer’s specifications' means non-prefabricated goods made on the basis of an individual choice or decision by the consumer;

(5) 'sales contract' means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services;

(6) 'service contract' means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof;

(7) 'distance contract' means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;

(8) 'off-premises contract' means any contract between the trader and the consumer:

(a) concluded in the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader;

(b) for which an offer was made by the consumer in the same circumstances as referred to in point (a);

(c) concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader in the simultaneous physical presence of the trader and the consumer;

(d) concluded during an excursion organised by the trader with the aim or effect of promoting and selling goods or services to the consumer;

(b) 'any movable retail premises where the trader carries out his activity on a usual basis';

(10) 'durable medium' means any instrument which enables the consumer or the trader to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(11) 'digital content' means data which are produced and stored in any form and which allow the unchanged reproduction of the information stored;

(12) 'financial service' means any service of a banking, credit, insurance, personal pension, investment or payment nature;

(13) 'public auction' means a method of sale where goods or services are offered by the trader to consumers, who attend or are given the possibility to attend the auction in person, through a transparent, competitive bidding procedure run by an auctioneer and where the successful bidder is bound to purchase the goods or services;

(14) 'commercial guarantee' means any undertaking by the trader or a producer (the guarantor) to the consumer, in addition to his legal obligation relating to the guarantee of conformity, to reimburse the price paid or to replace, repair or service goods in any way if they do not meet the specifications or any other requirements not related to conformity set out in the guarantee statement or in the relevant advertising available at the time of, or before the conclusion of the contract;

(15) 'ancillary contract' means a contract by which the consumer acquires goods or services related to a distance contract or an off-premises contract and where those goods are supplied or those services are provided by the trader or by a third party on the basis of an arrangement between that third party and the trader.
6. This Directive shall not prevent traders from offering consumers contractual arrangements which go beyond the protection provided for in this Directive.

Article 4
Level of harmonisation
Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more or less stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive.

CHAPTER II
CONSUMER INFORMATION FOR CONTRACTS OTHER THAN DISTANCE OR OFF-PREMISES CONTRACTS

Article 5
Information requirements for contracts other than distance or off-premises contracts
1. Before the consumer is bound by a contract other than a distance or an off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner, if that information is not already apparent from the context:
   (a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;
   (b) the identity of the trader, such as his trading name, the geographical address at which he is established and his telephone number;
   (c) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the fact that such additional charges may be payable;
   (d) where applicable, the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the service, and the trader's complaint handling policy;
   (e) in addition to a reminder of the existence of a legal guarantee of conformity for goods, the existence and the conditions of after-sales services and commercial guarantees, where applicable;
   (f) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;
   (g) where applicable, the functionality, including applicable technical protection measures, of digital content;
   (h) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. Member States shall not be required to apply paragraph 1 to contracts which involve day-to-day transactions and which are performed immediately at the time of their conclusion.

4. Member States may adopt or maintain additional pre-contractual information requirements for contracts to which this Article applies.

CHAPTER III
CONSUMER INFORMATION AND RIGHT OF WITHDRAWAL FOR DISTANCE AND OFF-PREMISES CONTRACTS

Article 6
Information requirements for distance and off-premises contracts
1. Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner:
   (a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;
   (b) the identity of the trader, such as his trading name;
   (c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;
   (d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;
   (e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall also include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;
   (f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;
   (g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;
   (h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11(1), as well as the model withdrawal form set out in Annex I(B);
   (i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;
   (j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14(3);
   (k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;
   (l) a reminder of the existence of a legal guarantee of conformity for goods;
   (m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;
   (n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable;
   (o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be
extended automatically, the conditions for terminating the contract;
(p) where applicable, the minimum duration of the consumer's obligations under the contract;
(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;
(r) where applicable, the functionality, including applicable technical protection measures, of digital content;
(s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of;
(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. In the case of a public auction, the information referred to in points (b), (c) and (d) of paragraph 1 may be replaced by the equivalent details for the auctioneer.

4. The information referred to in points (b), (i) and (j) of paragraph 1 may be provided by means of the model instructions on withdrawal set out in Annex I(1). The trader shall have fulfilled the information requirements laid down in points (b), (i) and (j) of paragraph 1 if he has supplied these instructions to the consumer, correctly filled in.

5. The information referred to in paragraph 1 shall form an integral part of the distance or off-premises contract and shall not be altered unless the contracting parties expressly agree otherwise.

6. If the trader has not complied with the information requirements on additional charges or other costs as referred to in point (e) of paragraph 1, or on the costs of returning the goods as referred to in point (j) of paragraph 1, the consumer shall not bear those charges or costs.

7. Member States may maintain or introduce in their national law language requirements regarding the contractual information, so as to ensure that such information is easily understood by the consumer.

8. The information requirements laid down in this Directive are in addition to information requirements contained in Directive 2006/123/EC and Directive 2000/31/EC and do not prevent Member States from imposing additional information requirements in accordance with those Directives.

Without prejudice to the first subparagraph, if a provision of Directive 2006/123/EC or Directive 2000/31/EC on the content and the manner in which the information is to be provided conflicts with a provision of this Directive, the provision of this Directive shall prevail.

9. As regards compliance with the information requirements laid down in this Chapter, the burden of proof shall be on the trader.

Article 7
Formal requirements for off-premises contracts
1. With respect to off-premises contracts, the trader shall give the information provided for in Article 6(1) to the consumer on paper or, if the consumer agrees, on another durable medium. That information shall be legible and in plain, intelligible language.

2. The trader shall provide the consumer with a copy of the signed contract or the confirmation of the contract on paper or, if the consumer agrees, on another durable medium, including, where applicable, the confirmation of the consumer's prior express consent and acknowledgement in accordance with point (m) of Article 16.

3. Where a consumer wants the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer makes such an express request on a durable medium.

4. With respect to off-premises contracts where the consumer has explicitly requested the services of the trader for the purpose of carrying out repairs or maintenance for which the trader and the consumer immediately perform their contractual obligations and where the payment to be made by the consumer does not exceed EUR 200:
(a) the trader shall, provide the consumer with the information referred to in points (b) and (c) of Article 6(1) and information about the price or the manner in which the price is to be calculated together with an estimate of the total price, on paper or, if the consumer agrees, on another durable medium. The trader shall provide the information referred to in points (a), (b) and (k) of Article 6(1), but may choose not to provide it on paper or another durable medium if the consumer expressly agrees;
(b) the confirmation of the contract provided in accordance with paragraph 2 of this Article shall contain the information provided for in Article 6(1).

Member States may decide not to apply this paragraph.

5. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 8
Formal requirements for distance contracts
1. With respect to distance contracts, the trader shall give the information provided for in Article 6(1) or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible.

2. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1).

The trader shall ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. If placing an order entails activating a button or a similar function, the button or similar function shall be labelled in an easily legible manner only with the words 'order with obligation to pay' or a corresponding unambiguous formulation indicating that placing the order entails an obligation to pay the trader. If the trader has not complied with this subparagraph, the consumer shall not be bound by the contract or order.

3. Trading websites shall indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

4. If the contract is concluded through a means of distance communication which allows limited space or time to display the information, the trader shall provide, on that particular means prior to the conclusion of such a contract, at least the pre-contractual information regarding the main characteristics of the goods or services, the identity of the trader, the total price, the right of withdrawal, the duration of the contract and, if the contract is of indeterminate duration, the conditions for terminating the contract, as referred to in points (a), (b), (e), (h) and (o) of Article 6(1). The other information referred to in Article 6(1) shall be provided by the trader or the consumer in an appropriate way in accordance with paragraph 1 of this Article.

5. Without prejudice to paragraph 4, if the trader makes a telephone call to the consumer with a view to concluding a distance contract, he shall, at the beginning of the conversation with the consumer, disclose his identity and,
where applicable, the identity of the person on whose behalf he makes that call, and the commercial purpose of the call.

6. Where a distance contract is to be concluded by telephone, Member States may provide that the trader has to confirm the offer to the consumer who is bound only once he has signed the offer or has sent his written consent. Member States may also provide that such confirmations have to be made on a durable medium.

7. The trader shall provide the consumer with the confirmation of the contract concluded, on a durable medium within a reasonable time after the conclusion of the distance contract, and at the latest at the time of the delivery of the goods or before the performance of the service begins. That confirmation shall include:

(a) all the information referred to in Article 6(1) unless the trader has already provided that information to the consumer on a durable medium prior to the conclusion of the distance contract; and
(b) where applicable, the confirmation of the consumer's prior express consent and acknowledgment in accordance with point (m) of Article 16.

8. Where a consumer wants the performance of services, or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer make an express request.

9. This Article shall be without prejudice to the provisions on the conclusion of e-contracts and the placing of e-orders set out in Articles 9 and 11 of Directive 2000/31/EC.

10. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 9

Right of withdrawal

1. Save where the exceptions provided for in Article 16 apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14.

2. Without prejudice to Article 10, the withdrawal period referred to in paragraph 1 of this Article shall expire after 14 days from:

(a) in the case of service contracts, the day of the conclusion of the contract;
(b) in the case of sales contracts, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the goods or:

(i) in the case of multiple goods ordered by the consumer in one order and delivered separately, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of each of the goods;
(ii) in the case of delivery of a good consisting of multiple lots or pieces, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last lot or piece;
(iii) in the case of contracts for regular delivery of goods during defined period of time, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the first good;
(c) in the case of contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium, the day of the conclusion of the contract.

3. The Member States shall not prohibit the contracting parties from performing their contractual obligations during the withdrawal period. Nevertheless, in the case of off-premises contracts, Member States may maintain existing national legislation prohibiting the trader from collecting the payment from the consumer during the given period after the conclusion of the contract.

Article 10

Omission of information on the right of withdrawal

1. If the trader has not provided the consumer with the information on the right of withdrawal as required by point (b) of Article 6(1), the withdrawal period shall expire 12 months from the end of the initial withdrawal period, as determined in accordance with Article 9(2).

2. If the trader has provided the consumer with the information provided for in paragraph 1 of this Article within 12 months from the day referred to in Article 9(2), the withdrawal period shall expire 14 days after the day upon which the consumer receives that information.

Article 11

Exercise of the right of withdrawal

1. Before the expiry of the withdrawal period, the consumer shall inform the trader of his decision to withdraw from the contract. For this purpose, the consumer may either:

(a) use the model withdrawal form as set out in Annex I(B); or
(b) make any other unequivocal statement setting out his decision to withdraw from the contract.

2. The consumer shall have exercised his right of withdrawal within the withdrawal period referred to in Article 9(2) and Article 10 if the communication concerning the exercise of the right of withdrawal is sent by the consumer before that period has expired.

3. The trader may, in addition to the possibilities referred to in paragraph 1, give the option to the consumer to electronically fill in and submit either the model withdrawal form set out in Annex I(B) or any other unequivocal statement on the trader's website. In those cases the trader shall communicate to the consumer an acknowledgement of receipt of such a withdrawal on a durable medium without delay.

4. The burden of proof of exercising the right of withdrawal in accordance with this Article shall be on the consumer.

Article 12

Effects of withdrawal

The exercise of the right of withdrawal shall terminate the obligations of the parties:

(a) to perform the distance or off-premises contract; or
(b) to conclude the distance or off-premises contract, in cases where an offer was made by the consumer.

Article 13

Obligations of the trader in the event of withdrawal

1. The trader shall reimburse all payments received from the consumer, including, if applicable, the costs of delivery without undue delay and in any event not later than 14 days from the day on which he is informed of the consumer's decision to withdraw from the contract in accordance with Article 11. The trader shall carry out the reimbursement referred to in the first subparagraph using the same means of payment as the consumer used for the initial transaction, unless the consumer indicates to the trader that he prefers to be reimbursed by means other than those means.

2. Notwithstanding paragraph 1, the trader shall not be required to reimburse the supplementary costs, if the consumer has expressly agreed otherwise and provided that the consumer does not incur any fees as a result of such reimbursement.
3. Unless the trader has offered to collect the goods himself, with regard to sales contracts, the trader may withhold the reimbursement until he has received the goods back, or until the consumer has supplied evidence of having sent back the goods, whichever is the earliest.

Article 14

Obligations of the consumer in the event of withdrawal

1. Unless the trader has offered to collect the goods himself, the consumer shall send back the goods or hand them over to the trader or to a person authorised by the trader to receive the goods, without undue delay and in any event not later than 14 days from the day on which he has communicated his decision to withdraw from the contract to the trader in accordance with Article 11. The deadline shall be met if the consumer sends back the goods before the period of 14 days has expired.

The consumer shall only bear the direct cost of returning the goods unless the trader has agreed to bear them or the trader failed to inform the consumer that the consumer has to bear them.

In the case of off-premises contracts where the goods have been delivered to the consumer's home at the time of the conclusion of the contract, the trader shall at his own expense collect the goods if, by their nature, those goods cannot normally be returned by post.

2. The consumer shall only be liable for any diminished value of the goods resulting from the handling of the goods other than what is necessary to establish the nature, characteristics and functioning of the goods. The consumer shall in any event not be liable for diminished value of the goods where the trader has failed to provide notice of the right of withdrawal in accordance with point (h) of Article 6(1).

3. Where a consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall pay to the trader an amount which is in proportion to what has been provided until the time the consumer has informed the trader of the exercise of the right of withdrawal, in comparison with the full coverage of the contract. The proportionate amount shall be paid by the consumer to the trader shall be calculated on the basis of the total price agreed in the contract. If the total price is excessive, the proportionate amount shall be calculated on the basis of the market value of what has been provided.

4. The consumer shall bear no cost for:

(a) the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, in full or in part, during the withdrawal period, where:
   (i) the trader has failed to provide information in accordance with points (h) or (j) of Article 6(1); or
   (ii) the consumer has not expressly requested performance to begin during the withdrawal period in accordance with Article 7(3) and Article 8(8); or

(b) the supply, in full or in part, of digital content which is not supplied on a tangible medium where:
   (i) the consumer has not given his prior express consent to the beginning of the performance before the end of the 14-day period referred to in Article 9;
   (ii) the consumer has not acknowledged that he loses his right of withdrawal when giving his consent; or
   (iii) the trader has failed to provide confirmation in accordance with Article 7(2) or Article 8(7).

5. Except as provided for in Article 13(2) and in this Article, the consumer shall not incur any liability as a consequence of the exercise of the right of withdrawal.

Effects of the exercise of the right of withdrawal on ancillary contracts

1. Without prejudice to Article 15 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers (20), if the consumer exercises his right of withdrawal from a distance or an off-premises contract in accordance with Articles 9 to 14 of this Directive, any ancillary contracts shall be automatically terminated, without any costs for the consumer, except as provided for in Article 13(2) and in Article 14 of this Directive.

2. The Member States shall lay down detailed rules on the termination of such contracts.

Article 16

Exceptions from the right of withdrawal

Member States shall not provide for the right of withdrawal set out in Articles 9 to 15 in respect of distance and off-premises contracts as regards the following:

(a) service contracts after the service has been fully performed if the performance has begun with the consumer’s prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader;

(b) the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period;

(c) the supply of goods made to the consumer’s specifications or clearly personalised;

(d) the supply of goods which are liable to deteriorate or expire rapidly;

(e) the supply of sealed goods which are not suitable for return due to health protection or hygiene reasons and were unsealed after delivery;

(f) the supply of goods which are, after delivery, according to their nature, inseparably mixed with other items;

(g) the supply of alcoholic beverages, the price of which has been agreed upon at the time of the conclusion of the sales contract, the delivery of which can only take place after 30 days and the actual value of which is dependent on fluctuations in the market which cannot be controlled by the trader;

(h) contracts where the consumer has specifically requested a visit from the trader for the purpose of carrying out urgent repairs or maintenance. If, on the occasion of such visit, the trader provides services in addition to those specifically requested by the consumer or goods other than replacement parts necessarily used for carrying out the maintenance or in making the repairs, the right of withdrawal shall apply to those additional services or goods;

(i) the supply of sealed audio or sealed video recordings or sealed computer software which were unsealed after delivery;

(j) the supply of a newspaper, periodical or magazine with the exception of subscription contracts for the supply of such publications;

(k) contracts concluded at a public auction;

(l) the provision of accommodation other than for residential purpose, transport of goods, car rental services, catering or services related to leisure activities if the contract provides for a specific date or period of performance;

(m) the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer’s prior express consent and his acknowledgment that he thereby loses his right of withdrawal.

CHAPTER IV

OTHER CONSUMER RIGHTS

Article 17

Scope

1. Articles 18 and 20 shall apply to sales contracts. Those Articles shall not apply to contracts for the supply of water,
gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or the supply of digital content which is not supplied on a tangible medium.

2. Articles 19, 21 and 22 shall apply to sales and service contracts and to contracts for the supply of water, gas, electricity, district heating or digital content.

Article 18

Delivery

1. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than 30 days from the conclusion of the contract.

2. Where the trader has failed to fulfill his obligation to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall call upon him to make the delivery within an additional period of time appropriate to the circumstances. If the trader fails to deliver the goods within that additional period of time, the consumer shall be entitled to terminate the contract.

The first subparagraph shall not be applicable to sales contracts where the trader has refused to deliver the goods or where delivery within the agreed delivery period is essential taking into account all the circumstances attending the conclusion of the contract or where the consumer informs the trader, prior to the conclusion of the contract, that delivery by or on a specified date is essential. In those cases, if the trader fails to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall be entitled to terminate the contract immediately.

3. Upon termination of the contract, the trader shall, without undue delay, reimburse all sums paid under the contract.

4. In addition to the termination of the contract in accordance with paragraph 2, the consumer may have recourse to other remedies provided for by national law.

Article 19

Fees for the use of means of payment

Member States shall prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such means.

Article 20

Passing of risk

In contracts where the trader dispatches the goods to the consumer, the risk of loss or of damage to the goods shall pass to the consumer when he or a third party indicated by the consumer and other than the carrier has acquired the physical possession of the goods. However, the risk shall pass to the consumer upon delivery to the carrier if the carrier was commissioned by the consumer to carry the goods and that choice was not offered by the trader, without prejudice to the rights of the consumer against the carrier.

Article 21

Communication by telephone

Member States shall ensure that where the trader operates a telephone line for the purpose of contacting him by telephone in relation to the contract concluded, the consumer, when contacting the trader is not bound to pay more than the basic rate. The first subparagraph shall be without prejudice to the right of telecommunication services providers to charge for such calls.

Article 22

Additional payments

Before the consumer is bound by the contract or offer, the trader shall seek the express consent of the consumer to any extra payment in addition to the remuneration agreed upon for the trader’s main contractual obligation. If the trader has not obtained the consumer’s express consent but has inferred it by using default options which the consumer is required to reject in order to avoid the additional payment, the consumer shall be entitled to reimbursement of this payment.

CHAPTER V

GENERAL PROVISIONS

Article 23

Enforcement

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive.

2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action under national law before the courts or before the competent administrative bodies to ensure that the national provisions transposing this Directive are applied:

(a) public bodies or their representatives;

(b) consumer organisations having a legitimate interest in protecting consumers;

(c) professional organisations having a legitimate interest in acting.

Article 24

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

2. Member States shall notify those provisions to the Commission by 13 December 2013 and shall notify it without delay of any subsequent amendment affecting them.

Article 25

Imperative nature of the Directive

If the law applicable to the contract is the law of a Member State, consumers may not waive the rights conferred on them by the national measures transposing this Directive. Any contractual terms which directly or indirectly waive or restrict the rights resulting from this Directive shall not be binding on the consumer.

Article 26

Information

Member States shall take appropriate measures to inform consumers and traders of the national provisions transposing this Directive and shall, where appropriate, encourage traders and code owners as defined in point (g) of Article 2 of Directive 2005/29/EC, to inform consumers of their codes of conduct.

Article 27

Inertia selling

The consumer shall be exempted from the obligation to provide any consideration in cases of unsolicited supply of goods, water, gas, electricity, district heating or digital content or unsolicited provision of services, prohibited by Article 5(5) and point 29 of Annex I to Directive 2005/29/EC. In such cases, the absence of a response from the consumer following such an unsolicited supply or provision shall not constitute consent.

Article 28

Transposition

1. Member States shall adopt and publish, by 13 December 2013, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of these measures.
in the form of documents. The Commission shall make use of these documents for the purposes of the report referred to in Article 30.

They shall apply those measures from 13 June 2014.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. The provisions of this Directive shall apply to contracts concluded after 13 June 2014.

Article 29
Reporting requirements
1. Where a Member State makes use of any of the regulatory choices referred to in Article 3(4), Article 6(7), Article 6(8), Article 7(4), Article 8(6) and Article 9(5), it shall inform the Commission thereof by 13 December 2013, as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.

Article 30
Reporting by the Commission and review
By 13 December 2016, the Commission shall submit a report on the application of this Directive to the European Parliament and the Council. That report shall include in particular an evaluation of the provisions of this Directive regarding digital content including the right of withdrawal.

The report shall be accompanied, where necessary, by legislative proposals to adapt this Directive to developments in the field of consumer rights.

CHAPTER VI
FINAL PROVISIONS

Article 31
Repeals

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex I.

Article 32
Amendment to Directive 93/13/EEC
In Directive 93/13/EEC, the following Article is inserted:

'Article 8a
1. Where a Member State adopts provisions in accordance with Article 8, it shall inform the Commission thereof, as well as of any subsequent changes, in particular where those provisions:

— extend the unfairness assessment to individually negotiated contractual terms or to the adequacy of the price or remuneration; or,

— contain lists of contractual terms which shall be considered as unfair.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.'

Article 33
Amendment to Directive 1999/44/EC
In Directive 1999/44/EC, the following Article is inserted:

'Article 8a
Reporting requirements
1. Where, in accordance with Article 8(2), a Member State adopts more stringent consumer protection provisions than those provided for in Article 5(1) to (3) and in Article 7(1), it shall inform the Commission thereof as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.'

Article 34
Entry into force
This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 35
Addressees
This Directive is addressed to the Member States.

Done at Strasbourg, 25 October 2011.

For the European Parliament
The President
J. BUSEK
For the Council
The President
M. DOWGIELEWICZ

(9) OJ L 88, 4.4.2011, p. 45.
(20) OJ L 133, 22.5.2008, p. 66.

ANNEX I
Information concerning the exercise of the right of withdrawal

A. Model instructions on withdrawal
Right of withdrawal
You have the right to withdraw from this contract within 14 days without giving any reason.

The withdrawal period will expire after 14 days from the day-

To exercise the right of withdrawal, you must inform us (1) of your decision to withdraw from this contract by an unequivocal statement (e.g. a letter sent by post, fax or e-
mail). You may use the attached model withdrawal form, but it is not obligatory.

To meet the withdrawal deadline, it is sufficient for you to send your communication concerning your exercise of the right of withdrawal before the withdrawal period has expired.

Effects of withdrawal

If you withdraw from this contract, we shall reimburse to you all payments received from you, including the costs of delivery (with the exception of the supplementary costs resulting from your choice of a type of delivery other than the least expensive type of standard delivery offered by us), without undue delay and in any event not later than 14 days from the day on which we are informed about your decision to withdraw from this contract. We will carry out such reimbursement using the same means of payment as you used for the initial transaction, unless you have expressly agreed otherwise; in any event, you will not incur any fees as a result of such reimbursement.

Instructions for completion:

Insert one of the following texts between inverted commas:

(a) in the case of a service contract or a contract for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium: ‘of the conclusion of the contract’;

(b) in the case of a sales contract: ‘on which you acquire, or a third party other than the carrier and indicated by you acquire, physical possession of the goods’;

(c) in the case of a contract relating to multiple goods ordered by the consumer in one order and delivered separately: ‘on which you acquire, or a third party other than the carrier and indicated by you acquire, physical possession of the last good’;

(d) in the case of a contract relating to delivery of a good consisting of multiple lots or pieces: ‘on which you acquire, or a third party other than the carrier and indicated by you acquire, physical possession of the last lot or piece’;

(e) in the case of a contract for regular delivery of goods during a defined period of time: ‘on which you acquire, or a third party other than the carrier and indicated by you acquire, physical possession of the first good’.

Insert your name, geographical address and, where available, your telephone number, fax number and e-mail address.

If you give the option to the consumer to electronically fill in and submit information about his withdrawal from the contract on your website, insert the following: ‘You can also electronically fill in and submit the model withdrawal form or any other unequivocal statement on our website [insert Internet address]. If you use this option, we will communicate to you an acknowledgement of receipt of such a withdrawal on a durable medium (e.g. by e-mail) without delay.’.

In the case of sales contracts in which you have not offered to collect the goods in the event of withdrawal, insert the following: ‘We may withhold reimbursement until we have received the goods back or you have supplied evidence of having sent back the goods, whichever is the earliest.’.

If the consumer has received goods in connection with the contract:

[a] insert:

ANNEX II
### ANNEX II

#### Correlation table

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 1</td>
<td>Article 3 read in conjunction with Article 2, points 8 and 9, and Article 16, point (b)</td>
<td></td>
</tr>
<tr>
<td>Article 1</td>
<td>Article 1 read in conjunction with Article 2, point 7</td>
<td></td>
</tr>
<tr>
<td>Article 2</td>
<td>Article 2, points 1 and 2</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 1</td>
<td>Article 2, point 7</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 2</td>
<td>Article 2, point 1</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 3</td>
<td>Article 2, point 2</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 4, first sentence</td>
<td>Article 2, point 7</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 4, second sentence</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 2, point 5</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 3(1)</td>
<td>Article 3(2), first indent</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), point (a)</td>
<td>Article 3(3), points (e) and (f)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), point (b)</td>
<td>Article 3(3), point (j)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), point (c)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), point (d)</td>
<td>Article 3(3), point (d)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), point (e)</td>
<td>Article 3(3), point (d)</td>
<td></td>
</tr>
<tr>
<td>Article 3(3)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 3(1), first indent</td>
<td>Article 3(3), point (d)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), second indent</td>
<td>Article 3(3), point (j)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), third indent</td>
<td>Article 3(3), point (m)</td>
<td></td>
</tr>
<tr>
<td>Article 3(3), fourth indent</td>
<td>Article 3(3), points (e) and (f)</td>
<td></td>
</tr>
<tr>
<td>Article 3(1), fifth indent</td>
<td>Article 6(3) and Article 16, point (k) read in conjunction with Article 2, point 13</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), first indent</td>
<td>Article 3(3), point (j)</td>
<td></td>
</tr>
<tr>
<td>Article 3(2), second indent</td>
<td>Article 3(3), point (f) (for rental of accommodation for residential purposes), point (g) (for package travel), point (h) (for timeshare), point (k) (for passenger transport with some exceptions) and Article 16, point (l) (exemption from the right of withdrawal)</td>
<td></td>
</tr>
<tr>
<td>Article 4, first sentence</td>
<td>Article 6(1), points (b), (c) and (h), and Article 7(1) and (2)</td>
<td></td>
</tr>
<tr>
<td>Article 4, second sentence</td>
<td>Article 6(1), point a and Article 7(1)</td>
<td></td>
</tr>
<tr>
<td>Article 4, third sentence</td>
<td>Article 6(1)</td>
<td></td>
</tr>
<tr>
<td>Article 4, fourth sentence</td>
<td>Article 10</td>
<td></td>
</tr>
<tr>
<td>Article 4(1), point (a)</td>
<td>Article 6(1), points (b) and (c)</td>
<td></td>
</tr>
<tr>
<td>Article 4(1), point (b)</td>
<td>Article 6(1), point (a)</td>
<td></td>
</tr>
<tr>
<td>Article 4(1), point (c)</td>
<td>Article 6(1), point (e)</td>
<td></td>
</tr>
<tr>
<td>Article 4(1), point (d)</td>
<td>Article 6(1), point (e)</td>
<td></td>
</tr>
<tr>
<td>Article 4(1)</td>
<td>Article 6(1), point (g)</td>
<td></td>
</tr>
<tr>
<td>Point (e)</td>
<td>Article 4(1), point (f)</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>Article 4(1), point (g)</td>
<td>Article 6(1), point (h)</td>
<td></td>
</tr>
<tr>
<td>Article 6(1)</td>
<td>Article 13 and Article 14(1), second and third subparagraphs</td>
<td></td>
</tr>
<tr>
<td>Article 6(2)</td>
<td>Article 7(1), Article 18(1) (for sales contracts)</td>
<td></td>
</tr>
<tr>
<td>Article 7(2)</td>
<td>Article 18(2), (3) and (4)</td>
<td></td>
</tr>
<tr>
<td>Article 7(3)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 8</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 9</td>
<td>Article 23(1)</td>
<td></td>
</tr>
<tr>
<td>Article 10</td>
<td>— (but see Article 13 of Directive 2002/58/EC)</td>
<td></td>
</tr>
<tr>
<td>Article 11(1)</td>
<td>Article 23(2)</td>
<td></td>
</tr>
<tr>
<td>Article 11(2)</td>
<td>Article 24(1)</td>
<td></td>
</tr>
<tr>
<td>Article 11(3), point (a)</td>
<td>Article 6(9) for the burden of proof concerning pre-contractual information; for the rest: —</td>
<td></td>
</tr>
<tr>
<td>Article 11(3), point (b)</td>
<td>Article 24(1)</td>
<td></td>
</tr>
<tr>
<td>Article 11(4)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 12</td>
<td>Article 3(2)</td>
<td></td>
</tr>
<tr>
<td>Article 12(1)</td>
<td>Article 25</td>
<td></td>
</tr>
<tr>
<td>Article 12(2)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 13</td>
<td>Article 30</td>
<td></td>
</tr>
<tr>
<td>Article 14</td>
<td>Article 28(1)</td>
<td></td>
</tr>
<tr>
<td>Article 15</td>
<td>Article 28(1)</td>
<td></td>
</tr>
<tr>
<td>Article 15(1)</td>
<td>Article 28(1)</td>
<td></td>
</tr>
<tr>
<td>Article 15(2)</td>
<td>Article 28(1)</td>
<td></td>
</tr>
<tr>
<td>Article 15(3)</td>
<td>Article 3(2)</td>
<td></td>
</tr>
<tr>
<td>Article 15(4)</td>
<td>Article 30</td>
<td></td>
</tr>
<tr>
<td>Article 16</td>
<td>Article 26</td>
<td></td>
</tr>
<tr>
<td>Article 17</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Article 18</td>
<td>Article 34</td>
<td></td>
</tr>
<tr>
<td>Article 19</td>
<td>Article 35</td>
<td></td>
</tr>
<tr>
<td>Article 5(1)</td>
<td>Articles 9 and 11</td>
<td></td>
</tr>
<tr>
<td>Article 5(2)</td>
<td>Article 12</td>
<td></td>
</tr>
</tbody>
</table>

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 169 thereof,
Having regard to the proposal from the European Commission, After transmission of the draft legislative act to the national Parliaments, Having regard to the opinion of the European Economic and Social Committee (1), Acting in accordance with the ordinary legislative procedure (2), Whereas:
(1) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through measures adopted pursuant to Article 114 TFEU. Article 38 of the Charter of Fundamental Rights of the European Union provides that Union policies are to ensure a high level of consumer protection.
(2) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services is ensured. The internal market should provide consumers with added value in the form of better quality, greater variety, reasonable prices and high safety standards for goods and services, which should promote a high level of consumer protection.
(3) Fragmentation of the internal market is detrimental to competitiveness, growth and job creation within the Union. Eliminating direct and indirect obstacles to the proper functioning of the internal market and improving citizens’ trust is essential for the completion of the internal market.
(4) Ensuring access to simple, efficient, fast and low-cost ways of resolving domestic and cross-border disputes which arise from sales or service contracts should benefit consumers and therefore boost their confidence in the market. That access should apply to online as well as to offline transactions, and is particularly important when consumers shop across borders.
(5) Alternative dispute resolution (ADR) offers a simple, fast and low-cost out-of-court solution to disputes between consumers and traders. However, ADR is not yet sufficiently and consistently developed across the Union. It is regrettable that, despite Commission Recommendations 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (3) and 2001/S/10/EC of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (4), ADR has not been correctly established and is not running satisfactorily in all geographical areas or business sectors in the Union. Consumers and traders are still not aware of the existing out-of-court redress mechanisms, with only a small percentage of citizens knowing how to file a complaint with an ADR entity. Where ADR procedures are available, their quality levels vary considerably in the Member States and cross-border disputes are often not handled effectively by ADR entities.
(6) The disparities in ADR coverage, quality and awareness in Member States constitute a barrier to the internal market and are among the reasons why many consumers abstain from shopping across borders and why they lack confidence that potential disputes with traders can be resolved in an easy, fast and inexpensive way. For the same reasons, traders might abstain from selling to consumers in other Member States where there is no sufficient access to high-quality ADR procedures. Furthermore, traders established in a Member State where high-quality ADR procedures are not sufficiently available are put at a competitive disadvantage with regard to traders that have access to such procedures and can thus resolve consumer disputes faster and more cheaply.
(7) In order for consumers to exploit fully the potential of the internal market, ADR should be available for all types of domestic and cross-border disputes covered by this Directive, ADR procedures should comply with consistent quality requirements that apply throughout the Union, and consumers and traders should be aware of the existence of such procedures. Due to increased cross-border trade and movement of persons, it is also important that ADR entities handle cross-border disputes effectively.
(8) As advocated by the European Parliament in its resolutions of 25 October 2011 on alternative dispute resolution in civil, commercial and family matters and of 20 May 2010 on delivering a single market to consumers and citizens, any holistic approach to the single market which delivers results for its citizens should as a priority develop simple, affordable, expedient and accessible system of redress. (9) In its Communication of 13 April 2011 entitled ‘Single Market Act — Twelve levers to boost growth and strengthen confidence — “Working together to create new growth”’, the Commission identified legislation on ADR which includes an electronic commerce (e-commerce) dimension, as one of the twelve levers to boost growth, strengthen confidence and make progress towards completing the Single Market.
(10) In its conclusions of 24-25 March and 23 October 2011, the European Council invited the European Parliament and the Council to adopt, by the end of 2012, a first set of priority
measures to bring a new impetus to the Single Market. Moreover, in its Conclusions of 30 May 2011 on the Priorities for relaunching the Single Market, the Council of the European Union highlighted the importance of e-commerce and agreed that consumer ADR schemes can offer low-cost, simple and quick redress for both consumers and traders. The successful implementation of those schemes requires sustained political commitment and support from all actors, without compromising the affordability, transparency, flexibility, speed and quality of decision-making by the ADR entities falling within the scope of this Directive.

(11) Given the increasing importance of online commerce and in particular cross-border trade as a pillar of Union economic activity, a properly functioning ADR infrastructure for consumer disputes and a properly integrated online dispute resolution (ODR) framework for consumer disputes arising from online transactions are necessary in order to achieve the Single Market Act’s aim of boosting citizens’ confidence in the internal market.

(12) This Directive and Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes (5) are two of interlinked and complementary legislative instruments. Regulation (EU) No 524/2013 provides for the establishment of an ODR platform which offers consumers and traders a single point of entry for the out-of-court resolution of online disputes, through ADR entities which are linked to the platform and offer ADR through quality ADR procedures. The availability of quality ADR entities across the Union is thus a precondition for the proper functioning of the ODR platform.

(13) This Directive should not apply to non-economic services of general interest. Non-economic services are services which are not performed for economic consideration. As a result, non-economic services of general interest performed by the State or on behalf of the State, without remuneration, should not be covered by this Directive irrespective of the legal form through which those services are provided.

(14) This Directive should not apply to health care services as defined in point (a) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare (6).

(15) The development within the Union of properly functioning ADR is necessary to strengthen consumers’ confidence in the internal market, including in the area of online commerce, and to fulfil the potential for and opportunities of cross-border and online trade. Such development should build on existing ADR procedures in the Member States and respect their legal traditions. Both existing and newly established properly functioning dispute resolution entities that comply with the quality requirements set out in this Directive should be considered as ‘ADR entities’ within the meaning of this Directive. The dissemination of ADR can also prove to be important in those Member States in which there is a substantial backlog of cases pending before the courts, preventing Union citizens from exercising their right to a fair trial within a reasonable time.

(16) This Directive should apply to disputes between consumers and traders concerning contractual obligations stemming from sales or services contracts, both online and offline, in all economic sectors, other than the exempted sectors. This should include disputes related to remedies arising from the sale or provision of digital content for remuneration. This Directive should apply to complaints submitted by consumers against traders. It should not apply to complaints submitted by traders against consumers or to disputes between traders, although it should not prevent Member States from adopting or maintaining in force provisions on procedures for the out-of-court resolution of such disputes.

(17) Member States should be permitted to maintain or introduce national provisions with regard to procedures not covered by this Directive, such as internal complaint handling procedures operated by the trader. Such internal complaint handling procedures can constitute an effective means for resolving consumer disputes at an early stage.

(18) The definition of ‘consumer’ should cover natural persons who are acting outside their trade, business, craft or profession. However, if the contract is concluded for purposes partly within and partly outside the person’s trade (dual purpose contracts) and the trade purpose is so limited as not to be predominant in the overall context of the supply, that person should also be considered as a consumer.

(19) Some existing Union legal acts already contain provisions concerning ADR. In order to ensure legal certainty, it should be provided that, in the event of conflict, this Directive is to prevail, except where it explicitly provides otherwise. In particular, this Directive should be without prejudice to Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters (7), which already sets out a framework for systems of mediation at Union level for cross-border disputes, without preventing the application of that Directive to internal mediation systems. This Directive is intended to apply horizontally to all types of ADR procedures, including to ADR procedures covered by Directive 2008/52/EC.

(20) ADR entities are highly diverse across the Union but also within the Member States. This Directive should cover any entity that is established on a durable basis, offers the resolution of a dispute between a consumer and a trader through an ADR procedure and is listed in accordance with this Directive. This Directive may also cover, if Member States so decide, dispute resolution entities which impose solutions which are binding on the parties. However, an out-of-court procedure which is created on an ad hoc basis for a single dispute between a consumer and a trader should not be considered as an ADR procedure for the purposes of this Directive.

(21) Also ADR procedures are highly diverse across the Union and within Member States. They can take the form of procedures where the ADR entity brings the parties together with the aim of facilitating an amicable solution, or procedures where the ADR entity proposes a solution or procedures where the ADR entity imposes a solution. They can also take the form of a combination of two or more such procedures. This Directive should be without prejudice to the form which ADR procedures take in the Member States.

(22) Procedures before dispute resolution entities where the natural persons in charge of dispute resolution are employed or receive any form of remuneration exclusively from the trader are likely to be exposed to a conflict of interest. Therefore, those procedures should, in principle, be excluded from the scope of this Directive, unless a Member State decides that such procedures can be recognised as ADR procedures under this Directive and provides that such entities are in complete conformity with the specific requirements on independence and impartiality laid down in this Directive. ADR entities offering dispute resolution through such procedures should be subject to regular evaluation of their compliance with the quality requirements set out in this Directive, including the specific additional requirements ensuring their independence.

(23) This Directive should not apply to procedures before consumer-complaint handling systems operated by the trader, nor to direct negotiations between the parties. Furthermore, it should not apply to attempts made by a judge to settle a dispute in the course of a judicial proceeding concerning that dispute.

(24) Member States should ensure that disputes covered by this Directive can be submitted to an ADR entity which complies with the requirements set out in this Directive and is listed in accordance with it. Member States should have the possibility of fulfilling this obligation by building on existing properly functioning ADR entities and adjusting their scope of application, if needed, or by providing for the creation of new ADR entities. This Directive should not preclude the functioning of existing dispute resolution entities operating within the framework of national consumer protection.
(25) This Directive should not prevent Member States from maintaining or introducing legislation on procedures for out-of-court resolution of consumer contractual disputes which is in compliance with the requirements set out in this Directive. Furthermore, in order to ensure that ADR entities can operate effectively, those entities should have the possibility of maintaining or introducing, in accordance with the laws of the Member State in which they are established, procedural rules that allow them to refuse to deal with disputes in specific circumstances, for example where a dispute is too complex and would therefore be better resolved in court. However, procedural rules allowing ADR entities to refuse to deal with a dispute should not impair significantly consumers' access to ADR procedures, including in the case of cross-border disputes. Thus, when providing for a monetary threshold, Member States should always take into account that the real value of a dispute may vary among Member States and, consequently, setting a disproportionately high threshold in one Member State could impair access to ADR procedures for consumers from other Member States. Member States should not be required to ensure that the consumer can submit his complaint to another ADR entity, where an ADR entity to which the complaint was first submitted has refused to deal with it because of its procedural rules. In such cases Member States should be deemed to have fulfilled their obligation to ensure full coverage of ADR entities.

(26) This Directive should allow traders established in a Member State to be covered by an ADR entity which is established in another Member State. In order to improve the coverage of and consumer access to ADR across the Union, Member States should have the possibility of deciding to rely on ADR entities established in another Member State or regional, transnational or pan-European ADR entities, where traders from different Member States are covered by the same ADR entity. Recourse to ADR entities established in another Member State or to transnational or pan-European ADR entities should, however, be without prejudice to Member States' responsibility to ensure full coverage by and access to ADR entities.

(27) This Directive should be without prejudice to Member States maintaining or introducing ADR procedures dealing jointly with identical or similar disputes between a trader and several consumers. Comprehensive impact assessments should be carried out on collective out-of-court settlements before such settlements are proposed at Union level. The existence of an effective system for collective claims and easy recourse to ADR should be complementary and they should not be mutually exclusive procedures.

(28) The processing of information relating to disputes covered by this Directive should comply with the rules on the protection of personal data laid down in the laws, regulations and administrative provisions of the Member States adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (8). Confidentiality and privacy should be respected at all times during the ADR procedure. Member States should be encouraged to protect the confidentiality of ADR procedures in any subsequent civil or commercial judicial proceedings or arbitration.

(30) Member States should nevertheless ensure that ADR entities make publicly available any systematic or significant problems that occur frequently and lead to disputes between consumers and traders. The information communicated in this regard could be accompanied by recommendations as to how such problems can be remedied or resolved in future, in order to raise traders' standards and to facilitate the exchange of information and best practices.

(31) Member States should ensure that ADR entities resolve disputes in a manner that is fair, practical and proportionate to both the consumer and the trader, on the basis of an objective assessment of the circumstances in which the complaint is made and with due regard to the rights of the parties.

(32) The independence and integrity of ADR entities is crucial in order to gain Union citizens' trust that ADR mechanisms will offer them a fair and independent outcome. The natural person or collegial body in charge of ADR should be independent of all those who might have an interest in the outcome and should have no conflict of interest which could impede him or it from reaching a decision in a fair, impartial and independent manner.

(33) The natural persons in charge of ADR should only be considered impartial if they cannot be subject to pressure that potentially influences their attitude towards the dispute. In order to ensure the independence of their actions, those persons should also be appointed for a sufficient duration, and should not be subject to any instructions from either party or their representative.

(34) In order to ensure the absence of any conflict of interest, natural persons in charge of ADR should disclose any circumstances that might affect their independence and impartiality or give rise to a conflict of interest with either party to the dispute they are asked to resolve. This could be any financial interest, direct or indirect, in the outcome of the ADR procedure or any personal or business relationship with one or more of the parties during the three years prior to assuming the post, including any capacity other than for the purposes of ADR in which the person concerned has acted for one or more of the parties, for a professional organisation or a business association of which one of the parties is a member or for any other member thereof.

(35) There is a particular need to ensure the absence of such pressure where the natural persons in charge of ADR are employed or receive any form of remuneration from the trader. Therefore, specific requirements should be provided for in the event that Member States decide to allow dispute resolution procedures in such cases to qualify as ADR procedures under this Directive. Where natural persons in charge of ADR are employed or receive any form of remuneration exclusively from a professional organisation or a business association of which the trader is a member, they should have at their disposal a separate and dedicated budget sufficient to fulfil their tasks.

(36) It is essential for the success of ADR, in particular in order to ensure the necessary trust in ADR procedures, that the natural persons in charge of ADR possess the necessary expertise, including a general understanding of law. In particular, those persons should have sufficient general knowledge of legal matters in order to understand the legal implications of the dispute, without being obliged to be a qualified legal professional.

(37) The applicability of certain quality principles to ADR procedures strengthens both consumers' and traders' confidence in such procedures. Such quality principles were first developed at Union level in Recommendations 98/257/EC and 2001/310/EC. By making some of the principles established in those Commission Recommendations binding, this Directive establishes a set of quality requirements which apply to all ADR procedures carried out by an ADR entity which has been notified to the Commission.

(38) This Directive should establish quality requirements of ADR entities, which should ensure the same level of protection and rights for consumers in both domestic and cross-border
disputes. This Directive should not prevent Member States from adopting or maintaining rules that go beyond what is provided for in this Directive.

(39) ADR entities should be accessible and transparent. In order to ensure the transparency of ADR entities and of ADR procedures it is necessary that the parties to a dispute, and anyone else who requests such information, receive the information they need in order to take an informed decision before engaging in an ADR procedure. The provision of such information to traders should not be required where their participation in ADR procedures is mandatory under national law.

(40) A properly functioning ADR entity should conclude online and offline dispute resolution proceedings expeditiously within a timeframe of 90 calendar days starting on the date on which the ADR entity has received the complete complaint file containing all relevant documentation pertaining to that complaint, and ending on the date on which the outcome of the ADR procedure is made available. The ADR entity which has received a complaint should notify the parties after receiving all the documents necessary to carry out the ADR procedure. In certain exceptional cases of a highly complex nature, including where one of the parties is unable, on justified grounds, to take part in the ADR procedure, ADR entities should be able to extend the timeframe for the purpose of undertaking an examination of the case in question. The parties should be informed of any such extension, and of the expected approximate length of time that will elapse before the conclusion of the procedure.

(41) ADR procedures should preferably be free of charge for the consumer. In the event that costs are applied, the ADR procedure should be accessible, attractive and inexpensive for consumers. To that end, costs should not exceed a nominal fee.

(42) ADR procedures should be fair so that the parties to a dispute are fully informed about their rights and the consequences of the choices they make in the context of an ADR procedure. ADR entities should inform consumers of their rights before they agree to or follow a proposed solution. Both parties should also be able to submit their information and evidence without being physically present.

(43) An agreement between a consumer and a trader to submit complaints to an ADR entity should not be binding on the consumer if it was concluded before the dispute has materialised and if it has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute. Furthermore, in ADR procedures which aim at resolving the dispute by imposing a solution, the solution imposed should be binding on the parties only if they were informed of its binding nature in advance and specifically accepted this. Specific acceptance by the trader concerned will be needed where their participation in ADR procedures is mandatory under national law.

(44) In ADR procedures which aim at resolving the dispute by imposing a solution on the consumer, in a situation where there is no conflict of laws, the solution imposed should not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State where the consumer and the trader are habitually resident. In a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 6(1) and (2) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the applicable law to contractual obligations (Rome I) (9), the solution imposed by the ADR entity should not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State in which the consumer is habitually resident. In a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 5(1) to (3) of the Rome Convention of 19 June 1980 on the law applicable to contractual obligations (10), the solution imposed by the ADR entity should not result in the consumer being deprived of the protection afforded to the consumer by the mandatory rules of the law of the Member State in which the consumer is habitually resident.

(45) The right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter of Fundamental Rights of the European Union. Therefore, ADR procedure rules should not be designed to replace court procedures and should not deprive consumers or traders of their rights to seek redress before the courts. This Directive should not prevent parties from exercising their right of access to the judicial system. In cases where a dispute could not be resolved through a given ADR procedure whose outcome is not binding, the parties should subsequently not be prevented from initiating judicial proceedings in relation to that dispute. Member States should be free to choose the appropriate means to achieve this objective. They should have the possibility to provide, inter alia, that limitation or prescription periods do not expire during an ADR procedure.

(46) In order to function efficiently, ADR entities should have sufficient human, material and financial resources at their disposal. Member States should decide on an appropriate form of funding for ADR entities on their territories, without restricting the funding of entities that are already operational. This Directive should be without prejudice to the question of whether ADR entities are publicly or privately funded or funded through a combination of public and private funding. However, ADR entities should be encouraged to specifically consider private forms of funding and to utilise public funds only at Member States’ discretion. This Directive should not affect the possibility for businesses or for professional organisations or business associations to fund ADR entities.

(47) When a dispute arises it is necessary that consumers are able to identify quickly which ADR entities are competent to deal with their complaint and to know whether or not the trader concerned will participate in proceedings submitted to an ADR entity. Traders who commit to use ADR entities to resolve disputes with consumers should inform consumers of the address and website of the ADR entity or entities by which they are covered. That information should be provided in a clear, comprehensible and easily accessible way on the trader’s website, where one exists, and if applicable in the general terms and conditions of sales or service contracts between the trader and the consumer. Traders should have the possibility of including on their websites, and in the terms and conditions of the relevant contracts, any additional information on their internal complaint handling procedures or on any other ways of directly contacting them with a view to settling disputes with consumers without referring them to an ADR entity. Where a dispute cannot be settled directly, the trader should provide the consumer, on paper or another durable medium, with the information on relevant ADR entities and specify if he will make use of them.

(48) The obligation on traders to inform consumers about the ADR entities by which those traders are covered should be without prejudice to provisions on consumer information on out-of-court redress procedures contained in other Union legal acts, which should apply in addition to the relevant information obligation provided for in this Directive.

(49) This Directive should not require the participation of traders in ADR procedures to be mandatory or the outcome of such procedures to be binding on traders, when a consumer has lodged a complaint against them. However, in order to ensure that consumers have access to redress and that they are not obliged to forego their claims, traders should be encouraged as far as possible to participate in ADR procedures. Therefore, this Directive should be without prejudice to any national rules making the participation of traders in such procedures mandatory or subject to incentives or sanctions or making their outcome binding on traders, provided that such legislation does not prevent the parties from exercising their right of access to the judicial system as provided for in Article 47 of the Charter of Fundamental Rights of the European Union.
(50) In order to avoid an unnecessary burden being placed on ADR entities, Member States should encourage consumers to contact the trader in an effort to solve the problem bilaterally before submitting a complaint to an ADR entity. In many cases, doing so would allow consumers to settle their disputes swiftly and at an early stage.

(51) Member States should involve the representatives of professional organisations, business associations and consumer organisations when developing ADR, in particular in relation to the principles of impartiality and independence.

(52) Member States should ensure that ADR entities cooperate on the resolution of cross-border disputes.

(53) Networks of ADR entities, such as the financial dispute resolution network 'FIN-NET' in the area of financial services, should be strengthened within the Union. Member States should encourage ADR entities to become part of such networks.

(54) Close cooperation between ADR entities and national authorities should strengthen the effective application of Union legal acts on consumer protection. The Commission and the Member States should facilitate cooperation between the ADR entities, in order to encourage the exchange of best practice and technical expertise and to discuss any problems arising from the operation of ADR procedures. Such cooperation should be supported, inter alia, through the Union’s forthcoming Consumer Programme.

(55) In order to ensure that ADR entities function properly and effectively, they should be closely monitored. For that purpose, each Member States should designate a competent authority or competent authorities which should perform that function. The Commission and competent authorities under this Directive should publish and update a list of ADR entities that comply with this Directive. Member States should ensure that ADR entities, the European Consumer Centre Network, and, where appropriate, the bodies designated in accordance with this Directive publish that list on their website by providing a link to the Commission’s website, and whenever possible on a durable medium at their premises. Furthermore, Member States should also encourage relevant consumer organisations and business associations to publish the list. Member States should also ensure the appropriate dissemination of information on what consumers should do if they have a dispute with a trader. In addition, competent authorities should publish regular reports on the development and functioning of ADR entities in their Member States. ADR entities should notify to competent authorities specific information on which those reports should be based. Member States should encourage ADR entities to provide such information using Commission Recommendation 2010/304/EU of 12 May 2010 on the use of a harmonised methodology for classifying and reporting consumer complaints and enquiries (11).

(56) It is necessary for Member States to lay down rules on penalties for infringements of the national provisions adopted to comply with this Directive and to ensure that those rules are implemented. The penalties should be effective, proportionate and dissuasive.

(57) Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) (12) should be amended to include a reference to this Directive in its Annex so as to reinforce cross-border cooperation on enforcement of this Directive.


(59) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents (14), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(60) Since the objective of this Directive, namely to contribute, through the achievement of a high level of consumer protection and without restricting consumers’ access to the courts, to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of proportionality, as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(61) This Directive respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and specifically Articles 7, 8, 38 and 47 thereof.

(62) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (15) and delivered an opinion on 12 January 2012 (16).

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter

The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by ensuring that consumers can, on a voluntary basis, submit complaints against traders to entities offering independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures. This Directive is without prejudice to national legislation making participation in such procedures mandatory, provided that such legislation does not prevent the parties from exercising their right of access to the judicial system.

Article 2

Scope

1. This Directive shall apply to procedures for the out-of-court resolution of domestic and cross-border disputes concerning contractual obligations stemming from sales contracts or service contracts between a trader established in the Union and a consumer resident in the Union through the intervention of an ADR entity which proposes or imposes a solution or brings the parties together with the aim of facilitating an amicable solution.

2. This Directive shall not apply to:

(a) procedures before dispute resolution entities where the natural persons in charge of dispute resolution are employed or remunerated exclusively by the individual trader, unless Member States decide to allow such procedures as ADR procedures under this Directive and the requirements set out in Chapter II, including the specific requirements of independence and transparency set out in Article 6(3), are met;

(b) procedures before consumer complaint-handling systems operated by the trader;

(c) non-economic services of general interest;

(d) disputes between traders;

(e) direct negotiation between the consumer and the trader;

(f) attempts made by a judge to settle a dispute in the course of a judicial proceeding concerning that dispute;

(g) procedures initiated by a trader against a consumer;
Article 3

Relationship with other Union legal acts

1. Save as otherwise set out in this Directive, if any provision of this Directive conflicts with a provision laid down in another Union legal act and relating to out-of-court redress procedures initiated by a consumer against a trader, the provision of this Directive shall prevail.

2. This Directive shall be without prejudice to Directive 2008/52/EC.

3. Article 13 of this Directive shall be without prejudice to provisions on consumer information on out-of-court redress procedures contained in other Union legal acts which shall apply in addition to that Article.

Article 4

Definitions

1. For the purposes of this Directive:
   (a) ‘consumer’ means any natural person who is acting for purposes which are outside his trade, business, craft or profession;
   (b) ‘trader’ means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;
   (c) ‘sales contract’ means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services;
   (d) ‘service contract’ means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof;
   (e) ‘domestic dispute’ means a contractual dispute arising from a sales or service contract where, at the time of the consumer, orders the goods or services, the consumer is resident in the same Member State as that in which the trader is established;
   (f) ‘cross-border dispute’ means a contractual dispute arising from a sales or service contract where, at the time of the consumer, the goods or services, the consumer is resident in a Member State other than the Member State in which the trader is established;
   (g) ‘ADR procedure’ means a procedure, as referred to in Article 2, which complies with the requirements set out in this Directive and is carried out by an ADR entity;
   (h) ‘ADR entity’ means any entity, however named or referred to, which is established on a durable basis and offers the right to his trade, business, craft or profession to his clients or other public body, at the place where it has its statutory seat, central administration or place of business, including a branch, agency or any other establishment.

2. A trader is established:
   (a) if the trader is a company or other legal person or association of natural or legal persons, where it has its statutory seat, central administration or place of business, including a branch, agency or any other establishment.

3. An ADR entity is established:
   (a) if it is operated by a natural person, at the place where it carries out ADR activities;
   (b) if the entity is operated by a legal person or association of natural or legal persons, at the place where that legal person or association of natural or legal persons carries out ADR activities or has its statutory seat;
   (c) if it is operated by an authority or other public body, at the place where that authority or other public body has its seat.

Chapter II

Access to and requirements applicable to ADR entities and ADR procedures

Article 5

Access to ADR entities and ADR procedures

1. Member States shall facilitate access by consumers to ADR procedures and shall ensure that disputes covered by this Directive and which involve a trader established on their respective territories can be submitted to an ADR entity which complies with the requirements set out in this Directive.

2. Member States shall ensure that ADR entities:
   (a) maintain an up-to-date website which provides the parties with easy access to information concerning the ADR procedure, and which enables consumers to submit a complaint and the requisite supporting documents online;
   (b) provide the parties, at their request, with the information referred to in point (a) on a durable medium;
   (c) where applicable, enable the consumer to submit a complaint offline;
   (d) enable the exchange of information between the parties via electronic means or, if applicable, by post;
   (e) accept both domestic and cross-border disputes, including disputes covered by Regulation (EU) No 524/2013; and
   (f) when dealing with disputes covered by this Directive, take the necessary measures to ensure that the processing of personal data complies with the rules on the protection of personal data laid down in the national legislation implementing Directive 95/46/EC in the Member State in which the ADR entity is established.

3. Member States may facilitate the admissibility of complaints submitted to an ADR entity, without prejudice to their responsibility to ensure full coverage and access to ADR entities.

4. Member States may, at their discretion, permit ADR entities to maintain and introduce procedural rules that allow them to refuse to deal with a given dispute on the grounds that:
   (a) the consumer did not attempt to contact the trader concerned in order to discuss his complaint and seek, as a first step, to resolve the matter directly with the trader;
   (b) the dispute is frivolous or vexatious;
   (c) the dispute is being or has previously been considered by another ADR entity or by a court;
   (d) the consumer has not submitted the complaint to the ADR entity within a pre-specified time limit, which shall not be set at less than one year from the date upon which the consumer submitted the complaint to the trader;
   (e) the consumer has not submitted the complaint to the ADR entity within a pre-specified monetary threshold;
   (f) the dispute with which the ADR entity deals is such as to seriously impair the effective operation of the ADR entity.

Where, in accordance with its procedural rules, an ADR entity is unable to consider a dispute that has been submitted to it,
that ADR entity shall provide both parties with a reasoned explanation of the grounds for not considering the dispute within three weeks of receiving the complaint file.

Such procedural rules shall not significantly impair consumers’ access to ADR procedures, including in the case of cross-border disputes.

5. Member States shall ensure that, when ADR entities are permitted to establish pre-specified monetary thresholds in order to limit access to ADR procedures, those thresholds are not set at a level at which they significantly impair the consumers’ access to complaint handling by ADR entities.

6. Where, in accordance with the procedural rules referred to in paragraph 4, an ADR entity is unable to consider a complaint that has been submitted to it, a Member State shall not be required to ensure that the consumer can submit his complaint to another ADR entity.

7. Where an ADR entity dealing with disputes in a specific economic sector is competent to consider disputes relating to a trader operating in that sector but which is not a member of the organisation or association forming or funding the ADR entity, the Member State shall be deemed to have fulfilled its obligations under paragraph 1 also with respect to disputes concerning that trader.

Article 6

Expertise, independence and impartiality

1. Member States shall ensure that the natural persons in charge of ADR possess the necessary expertise and are independent and impartial. This shall be guaranteed by ensuring that such persons:

(a) possess the necessary knowledge and skills in the field of alternative or judicial resolution of consumer disputes, as well as a general understanding of law;

(b) are appointed for a term of office of sufficient duration to ensure the independence of their actions, and are not liable to be relieved from their duties without just cause;

(c) are not subject to any instructions from either party or their representatives;

(d) are remunerated in a way that is not linked to the outcome of the procedure;

(e) without undue delay disclose to the ADR entity any circumstances that may, or may be seen to, affect their independence and impartiality or give rise to a conflict of interest with either party to the dispute they are asked to resolve. The obligation to disclose such circumstances shall be a continuing obligation throughout the ADR procedure. It shall not apply where the ADR entity comprises only one natural person.

2. Member States shall ensure that ADR entities have in place procedures to ensure that in the case of circumstances referred to in point (e) of paragraph 1:

(a) the natural person concerned is replaced by another natural person that shall be entrusted with conducting the ADR procedure; or failing that

(b) the natural person concerned refrains from conducting the ADR procedure and, where possible, the ADR entity proposes to the parties to submit the dispute to another ADR entity which is competent to deal with the dispute; or failing that

(c) the circumstances are disclosed to the parties and the natural person concerned is allowed to continue to conduct the ADR procedure only if the parties have not objected after they have been informed of the circumstances and their right to object.

This paragraph shall be without prejudice to point (a) of Article 9(2).

Where the ADR entity comprises only one natural person, only points (b) and (c) of the first subparagraph of this paragraph shall apply.

3. Where Member States decide to allow procedures referred to in point (a) of Article 2(2) as ADR procedures under this Directive, they shall ensure that, in addition to the general requirements set out in paragraphs 1 and 5, those procedures comply with the following specific requirements:

(a) the natural persons in charge of dispute resolution are nominated by, or form part of, a collegial body composed of an equal number of representatives of consumer organisations and of representatives of the trader and are appointed as a result of a transparent procedure;

(b) the natural persons in charge of dispute resolution are granted a period of office of a minimum of three years to ensure the independence of their actions;

(c) the natural persons in charge of dispute resolution commit not to work for the trader or a professional organisation or a business association of which the trader is a member for a period of three years after their position in the dispute resolution entity has ended;

(d) the dispute resolution entity does not have any hierarchical or functional link with the trader and is clearly separated from the trader’s operational entities and has a sufficient budget at its disposal, which is separate from the trader’s general budget, to fulfil its tasks.

This paragraph shall not apply where the natural persons concerned form part of a collegial body composed of an equal number of representatives of the professional organisation or business association by which they are employed or remunerated and of consumer organisations.

5. Member States shall ensure that ADR entities where the natural persons in charge of dispute resolution form part of a collegial body provide for an equal number of representatives of consumers’ interests and of representatives of traders’ interests in that body.

6. For the purposes of point (a) of paragraph 1, Member States shall encourage ADR entities to provide training for natural persons in charge of ADR. If such training is provided, competent authorities shall monitor the training schemes established by ADR entities, on the basis of information communicated to them in accordance with point (g) of Article 19(3).

Article 7

Transparency

1. Member States shall ensure that ADR entities make publicly available on their websites, on a durable medium upon request, and by any other means they consider appropriate, clear and easily understandable information on:

(a) their contact details, including postal address and e-mail address;

(b) the fact that ADR entities are listed in accordance with Article 20(2);

(c) the natural persons in charge of ADR, the method of their appointment and the length of their mandate;

(d) the expertise, impartiality and independence of the natural persons in charge of ADR, if they are employed or remunerated exclusively by the trader;

(e) their membership in networks of ADR entities facilitating cross-border dispute resolution, if applicable;

(f) the types of disputes they are competent to deal with, including any threshold if applicable;

(g) the procedural rules governing the resolution of a dispute and the grounds on which the ADR entity may refuse to deal with a given dispute in accordance with Article 5(4);

(h) the languages in which complaints can be submitted to the ADR entity and in which the ADR procedure is conducted;

(i) any preliminary requirements the parties may have to meet before an ADR procedure can be instituted, including the
requirement that an attempt be made by the consumer to
resolve the matter directly with the trader;
(k) whether or not the parties can withdraw from the
procedure;
(l) the costs, if any, to be borne by the parties, including any
rules on awarding costs at the end of the procedure;
(m) the average length of the ADR procedure;
(n) the legal effect of the outcome of the ADR procedure,
including the penalties for non-compliance in the case of a
decision having binding effect on the parties, if applicable;
(o) the enforceability of the ADR decision, if relevant.
2. Member States shall ensure that ADR entities make publicly
available on their websites, on a durable medium upon
request, and by any other means they consider appropriate,
annual activity reports. Those reports shall include the
following information relating to both domestic and cross-
border disputes:
(a) the number of disputes received and the types of
complaints to which they related;
(b) any systematic or significant problems that occur
frequently and lead to disputes between consumers and
traders; such information may be accompanied by
recommendations as to how such problems can be avoided or
resolved in future, in order to raise traders’ standards and to
facilitate the exchange of information and best practices;
(c) the rate of disputes the ADR entity has refused to deal with
and the percentage share of the types of grounds for such
refusal as referred to in Article 5(4);
(d) in the case of procedures referred to in point (a) of Article
2(2), the percentage shares of solutions proposed or imposed
in favour of the consumer and in favour of the trader, and of
disputes resolved by an amicable solution;
(e) the percentage share of ADR procedures which were
discontinued and, if known, the reasons for their
discontinuation;
(f) the average time taken to resolve disputes;
(g) the rate of compliance, if known, with the outcomes of the
ADR procedures;
(h) cooperation of ADR entities within networks of ADR
entities which facilitate the resolution of cross-border
disputes, if applicable.
Article 8
Effectiveness
Member States shall ensure that ADR procedures are effective
and fulfil the following requirements:
(a) the ADR procedure is available and easily accessible online
and offline to both parties irrespective of where they are;
(b) the parties have access to the procedure without being
obliged to retain a lawyer or a legal advisor, but the procedure
shall not deprive the parties of their right to independent
advice or to be represented or assisted by a third party at any
stage of the procedure;
(c) the ADR procedure is free of charge or available at a
nominal fee for consumers;
(d) the ADR entity which has received a complaint notifies the
parties to the dispute as soon as it has received all the
documents containing the relevant information relating to the
complaint;
(e) the outcome of the ADR procedure is made available
within a period of 90 calendar days from the date on which the
ADR entity has received the complete complaint file. In the
case of highly complex disputes, the ADR entity in charge may,
at its own discretion, extend the 90 calendar days’ time period.
The parties shall be informed of any extension of that period
and of the expected length of time that will be needed for the
conclusion of the dispute.
Article 9
Fairness
1. Member States shall ensure that in ADR procedures:
(a) the parties have the possibility, within a reasonable period of
time, of expressing their point of view, of being provided by
the ADR entity with the arguments, evidence, documents and
facts put forward by the other party, any statements made and
opinions given by experts, and of being able to comment on
them;
(b) the parties are informed that they are not obliged to retain
a lawyer or a legal advisor, but they may seek independent
advice or be represented or assisted by a third party at any
stage of the procedure;
(c) the parties are notified of the outcome of the ADR
procedure in writing or on a durable medium, and are given a
statement of the grounds on which the outcome is based.
2. In ADR procedures which aim at resolving the dispute by
proposing a solution, Member States shall ensure that:
(a) The parties have the possibility of withdrawing from the
procedure at any stage if they are dissatisfied with the
performance or the operation of the procedure. They shall be
informed of that right before the procedure commences.
Where national rules provide for mandatory participation by
the trader in ADR procedures, this point shall apply only to the
consumer.
(b) The parties, before agreeing or following a proposed
solution, are informed that:
(i) they have the choice as to whether or not to agree to or
follow the proposed solution;
(ii) participation in the procedure does not preclude the
possibility of seeking redress through court proceedings;
(iii) the proposed solution may be different from an outcome
determined by a court applying legal rules;
(c) The parties, before agreeing to or following a proposed
solution, are informed of the legal effect of agreeing to or
following such a proposed solution.
(d) The parties, before expressing their consent to a proposed
solution or amicable agreement, are allowed a reasonable
period of time to reflect.
3. Where, in accordance with national law, ADR procedures
provide that their outcome becomes binding on the trader
once the consumer has accepted the proposed solution, Article
9(2) shall be read as applicable only to the consumer.
Article 10
Liberty
1. Member States shall ensure that an agreement between a
consumer and a trader to submit complaints to an ADR entity
is not binding on the consumer if it was concluded before the
dispute has materialised and if it has the effect of depriving
the consumer of his right to bring an action before the courts
for the settlement of the dispute.
2. Member States shall ensure that in ADR procedures which
aim at resolving the dispute by imposing a solution the
solution imposed may be binding on the parties only if they
were informed of its binding nature in advance and
specifically accepted this. Specific acceptance by the trader is
not required if national rules provide that solutions are
binding on traders.
Article 11
Legality
1. Member States shall ensure that in ADR procedures which
aim at resolving the dispute by imposing a solution on the
consumer:
(a) in a situation where there is no conflict of laws, the
solution imposed shall not result in the consumer being
deprived of the protection afforded to him by the provisions
that cannot be derogated from by agreement by virtue of the
law of the Member State where the consumer and the trader
are habitually resident;
(b) in a situation involving a conflict of laws, where the law
applicable to the sales or service contract is determined in
accordance with Article 6(1) and (2) of Regulation (EC) No
593/2008, the solution imposed by the ADR entity shall not
result in the consumer being deprived of the protection
afforded to him by the provisions that cannot be derogated.
from by agreement by virtue of the law of the Member State in which he is habitually resident;
(c) in a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 5(1) to (3) of the Rome Convention of 19 June 1980 on the law applicable to contractual obligations, the solution imposed by the ADR entity shall not result in the consumer being deprived of the protection afforded to him by the mandatory rules of the law of the Member State in which he is habitually resident.
2. For the purposes of this Article, ‘habitual residence’ shall be determined in accordance with Regulation (EC) No 593/2008.

Article 12
Effect of ADR procedures on limitation and prescription periods
1. Member States shall ensure that parties who, in an attempt to settle a dispute, have recourse to ADR procedures the outcome of which is not binding, are not subsequently prevented from initiating judicial proceedings in relation to that dispute as a result of the expiry of limitation or prescription periods during the ADR procedure.
2. Paragraph 1 shall be without prejudice to provisions on limitation or prescription contained in international agreements to which Member States are party.

CHAPTER III
INFORMATION AND COOPERATION
Article 13
Consumer information by traders
1. Member States shall ensure that traders established on their territories inform consumers about the ADR entity or ADR entities by which those traders are covered, when those traders commit to or are obliged to use those entities to resolve disputes with consumers. That information shall include the website address of the relevant ADR entity or ADR entities.
2. The information referred to in paragraph 1 shall be provided in a clear, comprehensible and easily accessible way on the traders' website, where one exists, and, if applicable, in the general terms and conditions of sales or service contracts between the trader and a consumer.
3. Member States shall ensure that, in cases where a dispute between a consumer and a trader established in their territory could not be settled further to a complaint submitted directly by the consumer to the trader, the trader provides the consumer with the information referred to in paragraph 1, specifying whether he will make use of the relevant ADR entities to settle the dispute. That information shall be provided on paper or on another durable medium.

Article 14
Assistance for consumers
1. Member States shall ensure that, with regard to disputes arising from cross-border sales or service contracts, consumers can obtain assistance to access the ADR entity operating in another Member State which is competent to deal with their cross-border dispute.
2. Member States shall confer responsibility for the task referred to in paragraph 1 on their centres of the European Consumer Centre Network, on consumer organisations or on any other body.

Article 15
General information
1. Member States shall ensure that ADR entities, the centres of the European Consumer Centre Network and, where appropriate, the bodies designated in accordance with Article 14(2) make publicly available on their websites, by providing a link to the Commission's website, and whenever possible on a durable medium at their premises, the list of ADR entities referred to in Article 20(4).
2. Member States shall encourage relevant consumer organisations and business associations to make publicly available on their websites, and by any other means they consider appropriate, the list of ADR entities referred to in Article 20(4).
3. The Commission and Member States shall ensure appropriate dissemination of information on how consumers can access ADR procedures for resolving disputes covered by this Directive.
4. The Commission and the Member States shall take accompanying measures to encourage consumer organisations and professional organisations, at Union and at national level, to raise awareness of ADR entities and their procedures and to promote ADR take-up by traders and consumers. Those bodies shall also be encouraged to provide consumers with information about competent ADR entities when they receive complaints from consumers.

Article 16
Cooperation and exchanges of experience between ADR entities
1. Member States shall ensure that ADR entities cooperate in the resolution of cross-border disputes and conduct regular exchanges of best practices as regards the settlement of both cross-border and domestic disputes.
2. The Commission shall support and facilitate the networking of national ADR entities and the exchange and dissemination of their best practices and experiences.
3. Where a network of ADR entities facilitating the resolution of cross-border disputes exists in a sector-specific area within the Union, Member States shall encourage ADR entities that deal with disputes in that area to become a member of that network.
4. The Commission shall publish a list containing the names and contact details of the networks referred to in paragraph 3. The Commission shall, when necessary, update this list.

Article 17
Cooperation between ADR entities and national authorities enforcing Union legal acts on consumer protection
1. Member States shall ensure cooperation between ADR entities and national authorities entrusted with the enforcement of Union legal acts on consumer protection.
2. This cooperation shall in particular include mutual exchange of information on practices in specific business sectors about which consumers have repeatedly lodged complaints. It shall also include the provision of technical assessment and information by such national authorities to ADR entities where such assessment or information is necessary for the handling of individual disputes and is already available.
3. Member States shall ensure that cooperation and mutual information exchanges referred to in paragraphs 1 and 2 comply with the rules on the protection of personal data laid down in Directive 95/46/EC.
4. This Article shall be without prejudice to provisions on professional and commercial secrecy which apply to the national authorities enforcing Union legal acts on consumer protection. ADR entities shall be subject to rules of professional secrecy or other equivalent duties of confidentiality laid down in the legislation of the Member States where they are established.

CHAPTER IV
THE ROLE OF COMPETENT AUTHORITIES AND THE COMMISSION
Article 18
Designation of competent authorities
1. Each Member State shall designate a competent authority which shall carry out the functions set out in Articles 19 and 20. Each Member State may designate more than one competent authority. If a Member State does so, it shall
determine which of the competent authorities designated is the single point of contact for the Commission. Each Member State shall communicate the competent authority or, where appropriate, the competent authorities, including the single point of contact it has designated, to the Commission.

2. The Commission shall establish a list of the competent authorities including, where appropriate, the single point of contact communicated to it in accordance with paragraph 1, and publish that list in the Official Journal of the European Union.

Article 19
Information to be notified to competent authorities by dispute resolution entities

1. Member States shall ensure that dispute resolution entities established on their territories, which intend to qualify as ADR entities under this Directive and be listed in accordance with Article 20(2), notify to the competent authority the following:
   (a) their name, contact details and website address;
   (b) information on their structure and funding, including information on the natural persons in charge of dispute resolution, their remuneration, term of office and by whom they are employed;
   (c) their procedural rules;
   (d) their fees, if applicable;
   (e) the average length of the dispute resolution procedures;
   (f) the language or languages in which complaints can be submitted and the dispute resolution procedure conducted;
   (g) a statement on the types of disputes covered by the dispute resolution procedure;
   (h) the grounds on which the dispute resolution entity may refuse to deal with a given dispute in accordance with Article 5(4);
   (i) a reasoned statement on whether the entity qualifies as an ADR entity falling within the scope of this Directive and complies with the quality requirements set out in Chapter II.

2. Where Member States decide to allow procedures as referred to in point (a) to (b), ADR entities shall without undue delay notify those changes to the competent authority.

3. Member States shall ensure that ADR entities communicate to the competent authorities every two years information on:
   (a) the number of disputes received and the types of complaints to which they related;
   (b) the percentage share of ADR procedures which were discontinued before an outcome was reached;
   (c) the average time taken to resolve the disputes received;
   (d) the rate of compliance, if known, with the outcomes of the ADR procedures;
   (e) any systematic or significant problems that occur frequently and lead to disputes between consumers and traders. The information communicated in this regard may be accompanied by recommendations as to how such problems can be avoided or resolved in future;
   (f) where applicable, an assessment of the effectiveness of their cooperation within networks of ADR entities facilitating the resolution of cross-border disputes;
   (g) where applicable, the training provided to natural persons in charge of ADR in accordance with Article 6(6);
   (h) an assessment of the effectiveness of the ADR procedure offered by the entity and of possible ways of improving its performance.

Article 20
Role of the competent authorities and of the Commission

1. Each competent authority shall assess, in particular on the basis of the information it has received in accordance with Article 19(1), whether the dispute resolution entities notified to it qualify as ADR entities falling within the scope of this Directive and comply with the quality requirements set out in Chapter II and in national provisions implementing it, including national provisions going beyond the requirements of this Directive, in conformity with Union law.

2. Each competent authority shall, on the basis of the assessment referred to in paragraph 1, list all the ADR entities that have been notified to it and fulfil the conditions set out in paragraph 1.

That list shall include the following:
   (a) the name, the contact details and the website addresses of the ADR entities referred to in the first subparagraph;
   (b) their fees, if applicable;
   (c) the language or languages in which complaints can be submitted and the ADR procedure conducted;
   (d) the types of disputes covered by the ADR procedure;
   (e) the sectors and categories of disputes covered by each ADR entity;
   (f) the need for the physical presence of the parties or of their representatives, if applicable, including a statement by the ADR entity on whether the ADR procedure is open to be conducted as an oral or a written procedure;
   (g) the binding or non-binding nature of the outcome of the procedure and the grounds on which the ADR entity may refuse to deal with a given dispute in accordance with Article 5(4).

Each competent authority shall notify the list referred to in the first subparagraph of this paragraph to the Commission. If any changes are notified to the competent authority in accordance with the second subparagraph of Article 19(1), that list shall be updated without undue delay and the relevant information notified to the Commission.

If a dispute resolution entity listed as an ADR entity under this Directive no longer complies with the requirements referred to in paragraph 1, the competent authority concerned shall contact that dispute resolution entity, stating the requirements the dispute resolution entity fails to comply with and requesting it to ensure compliance immediately. If the dispute resolution entity after a period of three months still does not fulfil the requirements referred to in paragraph 1, the competent authority shall remove the dispute resolution entity from the list referred to in the first subparagraph of this paragraph. That list shall be updated without undue delay and the relevant information notified to the Commission.

If a Member State has designated more than one competent authority, the list and its updates referred to in paragraph 3 shall be notified to the Commission by the single point of contact referred to in Article 18(1). That list and those updates shall relate to all ADR entities established in that Member State.

4. The Commission shall establish a list of the ADR entities notified to it in accordance with paragraph 2 and update that list whenever changes are notified to the Commission. The Commission shall make publicly available that list and its updates on its website and on a durable medium. The Commission shall transmit that list and its updates to the competent authorities. Where a Member State has designated a single point of contact in accordance with Article 18(1), the Commission shall transmit that list and its updates to the single point of contact.

5. Each competent authority shall make publicly available the consolidated list of ADR entities referred to in paragraph 4 on its website by providing a link to the relevant Commission website. In addition, each competent authority shall make publicly available that list and its updates on a durable medium.

6. By 9 July 2018, and every four years thereafter, each competent authority shall publish and send to the Commission a report on the development and functioning of ADR entities. That report shall in particular:
   (a) identify best practices of ADR entities;

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Article 100 A thereof,
Having regard to the proposal from the Commission (1),
In cooperation with the European Parliament (2),
Having regard to the opinion of the Economic and Social Committee (3),
Whereas it is necessary to adopt measures with the aim of progressively establishing the internal market before 31 December 1992; whereas the internal market comprises an area without internal frontiers in which goods, persons, services and capital move freely;
Whereas the laws of Member States relating to the terms of contract between the seller of goods or supplier of services, on the one hand, and the consumer of them, on the other hand, show many disparities, with the result that the national markets for the sale of goods and services to consumers differ from each other and that distortions of competition may arise amongst the sellers and suppliers, notably when they sell and supply in other Member States;
Whereas, in particular, the laws of Member States relating to unfair terms in consumer contracts show marked divergences; whereas it is the responsibility of the Member States to ensure that contracts concluded with consumers do not contain unfair terms;
Whereas, generally speaking, consumers do not know the rules of law which, in Member States other than their own, govern contracts for the sale of goods or services; whereas this lack of awareness may deter them from direct transactions for the purchase of goods or services in another Member State;
Whereas in order to facilitate the establishment of the internal market and to safeguard the citizen in his role as consumer when acquiring goods and services under contracts which are governed by the laws of Member States other than his own, it is essential to remove unfair terms from those contracts;
Whereas sellers of goods and suppliers of services will thereby be helped in their task of selling goods and supplying services, both at home and throughout the internal market; whereas competition will thus be stimulated, so contributing to increased choice for Community citizens as consumers;
Whereas the two Community programmes for a consumer protection and information policy (4) underlined the importance of safeguarding consumers in the matter of unfair terms of contract; whereas this protection ought to be provided by laws and regulations which are either harmonized at Community level or adopted directly at that level;
Whereas in accordance with the principle laid down under the heading 'Protection of the economic interests of the consumers', as stated in those programmes: 'acquirers of goods and services should be protected against the abuse of power by the seller or supplier, in particular against one-sided standard contracts and the unfair exclusion of essential rights in contracts';
Whereas more effective protection of the consumer can be achieved by adopting uniform rules of law in the matter of unfair terms; whereas those rules should apply to all contracts concluded between sellers or suppliers and consumers; whereas as a result inter alia contracts relating to employment, contracts relating to succession rights, contracts relating to rights under family law and contracts relating to the incorporation and organization of companies or partnership agreements must be excluded from this Directive;
Whereas the consumer must receive equal protection under contracts concluded by word of mouth and written contracts regardless, in the latter case, of whether the terms of the contract are contained in one or more documents;
Whereas, however, as they now stand, national laws allow only partial harmonization to be envisaged; whereas, in particular, only contractual terms which have not been individually negotiated are covered by this Directive; whereas Member States should have the option, with due regard for the Treaty, to afford consumers a higher level of protection through national provisions that are more stringent than those of this Directive;
Whereas the statutory or regulatory provisions of the Member States which directly or indirectly determine the terms of consumer contracts are presumed not to contain unfair terms; whereas, therefore, it does not appear to be necessary to subject the terms which reflect mandatory statutory or regulatory provisions and the principles or provisions of international conventions to which the Member States or the Community are party; whereas in that respect the wording 'mandatory statutory or regulatory provisions' in Article 1 (2) also covers rules which, according to the law, shall apply between the contracting parties provided that no other arrangements have been established;
Whereas Member States must however ensure that unfair terms are not included, particularly because this Directive also applies to trades, business or professions of a public nature;
Whereas it is necessary to fix in a general way the criteria for assessing the unfair character of contract terms;
Whereas the assessment, according to the general criteria chosen, of the unfair character of terms, in particular in sale or supply activities of a public nature providing collective services which take account of solidarity among users, must be supplemented by a means of making an overall evaluation of the different interests involved; whereas this constitutes the requirement of good faith; whereas, in making an assessment of good faith, particular regard shall be had to the strength of the bargaining positions of the parties, whether the consumer had an inducement to agree to the term and whether the goods or services were supplied to the special order of the consumer; whereas the requirement of good faith may be satisfied by the seller or supplier where he deals fairly and equitably with the other party whose legitimate interests he has to take into account;
Whereas, for the purposes of this Directive, the annexed list of terms can be of indicative value only and, because of the cause of the minimal character of the Directive, the scope of these terms may be the subject of amplification or more restrictive editing by the Member States in their national laws;
Whereas the nature of goods or services should have an influence on assessing the unfairness of contractual terms;
Whereas, for the purposes of this Directive, assessment of unfair character shall not be made of terms which describe the main subject matter of the contract nor the quality/price ratio of the goods or services supplied; whereas the main subject matter of the contract and the price/quality ratio may nevertheless be taken into account in assessing the fairness of other terms; whereas it follows, inter alia, that in insurance contracts, the terms which clearly define or circumscribe the insured risk and the insurer's liability shall not be subject to such assessment since these restrictions are taken into account in calculating the premium paid by the consumer;
Whereas contracts should be drafted in plain, intelligible language, the consumer should actually be given an opportunity to examine all the terms and, if in doubt, the interpretation most favourable to the consumer should prevail;
Whereas Member States should ensure that unfair terms are not used in contracts concluded with consumers by a seller or supplier and that if, nevertheless, such terms are so used, they will not bind the consumer, and the contract will continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair provisions;
Whereas there is a risk that, in certain cases, the consumer may be deprived of protection under this Directive by designating the law of a non-Member country as the law applicable to the contract; whereas provisions should therefore be included in this Directive designed to avert this risk;
Whereas persons or organizations, if regarded under the law of a Member State as having a legitimate interest in the matter, must have facilities for initiating proceedings concerning terms of contract drawn up for general use in contracts concluded with consumers, and in particular unfair terms, either before a court or before an administrative authority competent to decide upon complaints or to initiate
Article 1
1. The purpose of this Directive is to approximate the laws, regulations and administrative provisions of the Member States relating to unfair terms in contracts concluded between a seller or supplier and a consumer.
2. The contractual terms which reflect mandatory statutory or regulatory provisions and the provisions or principles of international conventions to which the Member States or the Community are party, particularly in the transport area, shall not be subject to the provisions of this Directive.

Article 2
For the purposes of this Directive:
(a) ‘unfair terms’ means the contractual terms defined in Article 3;
(b) ‘consumer’ means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession;
(c) ‘seller or supplier’ means any natural or legal person who, in contracts covered by this Directive, is acting for purposes relating to his trade, business or profession, whether publicly owned or privately owned.

Article 3
1. A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer.
2. A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.

Article 4
1. Without prejudice to Article 7, the unfairness of a contractual term shall be assessed, taking into account the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent.
2. Assessment of the unfair nature of the terms shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration, on the one hand, as against the services or goods supplied in exchange, on the other, in so far as these terms are in plain intelligible language.

Article 5
In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7 (2).

Article 6
1. Member States shall lay down that unfair terms used in a contract concluded with a consumer by a seller or supplier shall, as provided for under their national law, not be binding on the consumer and that the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms.
2. Member States shall take the necessary measures to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of the Member States.

Article 7
1. Member States shall ensure that, in the interests of consumers and of competitors, adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers.
2. The means referred to in paragraph 1 shall include provisions whereby persons or organizations, having a legitimate interest under national law in protecting consumers, may take action according to the national law concerned before the courts or before competent administrative bodies for a decision as to whether contractual terms drawn up for general use are unfair, so that they can apply appropriate and effective means to prevent the continued use of such terms.
3. With due regard for national laws, the legal remedies referred to in paragraph 2 may be directed separately or jointly against a number of sellers or suppliers from the same economic sector or their associations which use or recommend the use of the same general contractual terms or similar terms.

Article 8
Member States may adopt or retain the most stringent provisions compatible with the Treaty in the area covered by this Directive, to ensure a maximum degree of protection for the consumer.

Article 8a
1. Where a Member State adopts provisions in accordance with Article 8, it shall inform the Commission thereof, as well as of any subsequent changes, in particular where those provisions:
   — extend the unfairness assessment to individually negotiated contractual terms or to the adequacy of the price or remuneration;
   — contain lists of contractual terms which shall be considered as unfair;
2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.
3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.

Article 9
The Commission shall present a report to the European Parliament and to the Council concerning the application of this Directive five years at the latest after the date in Article 10 (1).

Article 10
Article 11

This Directive is addressed to the Member States.

Done at Luxembourg, 5 April 1993.

For the Council

The President

N. HELVEG PETERSEN

(3) OJ No C 159, 17. 6. 1991, p. 34.

ANNEX

TERMS REFERRED TO IN ARTICLE 3 (3) 1. Terms which have the object or effect of:

(a) excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;

(b) inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, including the option of offsetting a debt owed to the seller or supplier against any claim which the consumer may have against him;

(c) making an agreement binding on the consumer whereas provision of services by the seller or supplier is subject to a condition whose realization depends on his own will alone;

(d) permitting the seller or supplier to retain sums paid by the consumer where the latter decides not to conclude or perform the contract, without providing for the consumer to receive compensation of an equivalent amount from the seller or supplier where the latter is the party cancelling the contract;

(e) requiring any consumer who fails to fulfil his obligations where the seller or supplier does not perform his;

(f) authorizing the seller or supplier to dissolve the contract on a discretionary basis where the facility is not granted to the consumer, or permitting the seller or supplier to retain the sums paid for services not yet supplied by him where it is the seller or supplier himself who dissolves the contract;

(g) enabling the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so;

(h) automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early;

(i) irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract;

(j) enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;

(k) enabling the seller or supplier to alter unilaterally without a valid reason any characteristics of the product or service to be provided;

(l) providing for the price of goods to be determined at the time of delivery or allowing a seller of goods or supplier of services to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded;

(m) giving the seller or supplier the right to determine whether the goods or services supplied are in conformity with the contract, or giving him the exclusive right to interpret any term of the contract;

(n) limiting the seller's or supplier's obligation to respect commitments undertaken by his agents or making his commitments subject to compliance with a particular formality;

(o) obliging the consumer to fulfil all his obligations where the seller or supplier does not perform his;

(p) giving the seller or supplier the possibility of transferring his rights and obligations under the contract, where this may serve to reduce the guarantees for the consumer, without the latter's agreement;

(q) excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.

2. Scope of subparagraphs (g), (j) and (l)

(a) Subparagraph (g) is without hindrance to terms by which a supplier of financial services reserves the right to terminate unilaterally a contract of indeterminate duration without notice where there is a valid reason, provided that the supplier is required to inform the other contracting party or parties thereof immediately.

(b) Subparagraph (j) is without hindrance to terms under which a supplier of financial services reserves the right to alter unilaterally without a valid reason any characteristics of the product or service to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded, provided that he is required to inform the consumer of the change and the latter is free to dissolve the contract immediately.

Subparagraph (l) is also without hindrance to terms under which a supplier of financial services reserves the right to alter unilaterally the conditions of a contract of indeterminate duration, provided that he is required to inform the consumer with reasonable notice and that the consumer is free to dissolve the contract.

(c) Subparagraphs (g), (j) and (l) do not apply to:

- transactions in transferable securities, financial instruments and other products or services where the price is linked to fluctuations in a stock exchange quotation or index or a financial market rate that the seller or supplier does not control;

- contracts for the purchase or sale of foreign currency, traveller's cheques or international money orders denominated in foreign currency;

(d) Subparagraph (j) is without hindrance to price-indexation clauses, where lawful, provided that the method by which prices vary is explicitly described.

Relevant case law on unfair terms in consumer contracts
Summary of the Judgment


1. Article 6(1) of Council Directive 93/13 on unfair terms in consumer contracts must be interpreted as meaning that an unfair contract term is not binding on the consumer, and it is not necessary, in that regard, for that consumer to have successfully contested the validity of such a term beforehand.

The aim of Article 6 of that directive, which is to strengthen consumer protection, would not be achieved if the consumer were himself obliged to raise the unfairness of contractual terms. In addition, effective protection of the consumer may be attained only if the national court acknowledges that it has power to evaluate terms of this kind of its own motion. (see paras 23, 28, operative part 1)

2. The national court is required to examine, of its own motion, the unfairness of a contractual term where it has available to it the legal and factual elements necessary for that task, Where it considers such a term to be unfair, it must not apply it, except if the consumer opposes that non-application.

That duty is also incumbent on the national court when it is ascertaining its own territorial jurisdiction.

The court seised of the action is required to ensure the effectiveness of the protection intended to be given by the provisions of Directive 93/13 on unfair terms in consumer contracts. Consequently, the role thus attributed to the national court by Community law in this area is not limited to a mere power to rule on the possible unfairness of a contractual term, but also consists of the obligation to examine that issue of its own motion, where it has available to it the legal and factual elements necessary for that task, including when it is assessing whether it has territorial jurisdiction. In carrying out that obligation, the national court is, however, required under that directive to exclude the possibility that the term in question may be applicable, if the consumer, after having been informed of it by that court, does not intend to assert its unfair or non-binding status. (see paras 32-33, 35, operative part 2)

3. It is for the national court to determine whether a contractual term, such as a term conferring jurisdiction, satisfies the criteria to be categorised as unfair within the meaning of Article 3(1) of Directive 93/13 on unfair terms in consumer contracts. In so doing, the national court must take account of the fact that a term, contained in a contract concluded between a consumer and a seller or supplier, which has been included without being individually negotiated and which confers exclusive jurisdiction on the court in the territorial jurisdiction of which the seller or supplier has his principal place of business, may be considered to be unfair. (see para. 44, operative part 3)
with Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities(4), a high level of Community integration is achieved.

(5) The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services; these obstacles arise from divergence in regulation and from legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas, obstacles might be justified in the light of the case-law of the Court of Justice of the European Communities; legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State.

(6) In the light of Community objectives, of Articles 43 and 49 of the Treaty and of secondary Community law, these obstacles should be eliminated by coordinating certain national laws and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market; by dealing only with certain specific matters which give rise to problems for the internal market, this Directive is fully consistent with the need to respect the principle of subsidiarity as set out in Article 5 of the European Parliament.

(7) In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.

(8) The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such.

(9) The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

(10) In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the protection of public health; according to Article 152 of the Treaty, the protection of public health is an essential component of other Community policies.


(12) It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not prejudice any instruments which might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed on a large number of the services covered by this Directive, must be excluded from the scope of this Directive.

(13) This Directive does not aim to establish rules on fiscal obligations nor does it pre-empt the drawing up of Community instruments concerning fiscal aspects of electronic commerce.

(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of personal data and the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

(15) The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others.
than the senders and receivers, except when legally authorised.

(16) The exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value; this does not cover promotional competitions or games where the purpose is to encourage the sale of goods or services and where payments, if they arise, serve only to acquire the promoted goods or services.

(17) The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(21) and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access(22); this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service; those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition.

(18) Information society services span a wide range of economic activities which take place on-line; these activities can consist of selling goods such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

(19) The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.

(20) The definition of "recipient of a service" covers all types of usage of information society services; both by persons who provide information on open networks such as the Internet and by persons who make use of information on the Internet for private or professional reasons.

(21) The scope of the coordinated field is without prejudice to future Community harmonisation relating to information society services and to future legislation adopted at national level in accordance with the principle that the concept of "establishment" involves the actual pursuit of economic activities which take place on-line; the coordinated field covers only requirements relating to on-line activities such as on-line information, on-line advertising, on-line shopping, on-line contracting and does not concern Member States' legal requirements relating to goods such as safety standards, labelling obligations, or liability for goods, or Member States' requirements relating to the transport of goods, including the distribution of medicinal products; the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

(22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States it is essential to establish, in the state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

(20) The definition of "recipient of a service" covers all types of usage of information society services; both by persons who provide information on open networks such as the Internet and by persons who make use of information on the Internet for private or professional reasons.

(21) The scope of the coordinated field is without prejudice to future Community harmonisation relating to information society services and to future legislation adopted at national level in accordance with the principle that the concept of "establishment" involves the actual pursuit of economic activities which take place on-line; the coordinated field covers only requirements relating to on-line activities such as on-line information, on-line advertising, on-line shopping, on-line contracting and does not concern Member States' legal requirements relating to goods such as safety standards, labelling obligations, or liability for goods, or Member States' requirements relating to the transport of goods, including the distribution of medicinal products; the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

(22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States it is essential to establish, in the state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.
consisting of the physical delivery of a printed electronic mail message and does not affect voluntary accreditation systems, in particular for providers of electronic signature certification service.

(29) Commercial communications are essential for the financing of information society services and for developing a wide variety of new, charge-free services; in the interests of consumer protection and fair trading, commercial communications, including discounts, promotional offers and promotional competitions or games, must meet a number of transparency requirements; these requirements are without prejudice to Directive 97/7/EC; this Directive should not affect existing Directives on commercial communications, in particular Directive 98/43/EC.

(30) The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; the question of consent by recipient of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed, in particular, by Directive 97/7/EC and by Directive 97/66/EC; in Member States which authorize unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communications are clearly identifiable as such and that they are regulated and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

(31) Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent by recipients must ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

(32) In order to remove barriers to the development of cross-border services within the Community which members of the regulated professions might offer on the Internet, it is necessary that compliance be guaranteed at Community level with professional rules aiming, in particular, to protect consumers or public health; codes of conduct at Community level would be the best means of determining the rules on professional ethics applicable to commercial communication; the drawing-up or, where appropriate, the adaptation of such rules should be encouraged without prejudice to the autonomy of professional bodies and associations.

(33) This Directive complements Community law and national law relating to regulated professions maintaining a coherent set of applicable rules in this field.

(34) Each Member State is to amend its legislation containing requirements, and in particular requirements as to form, which are likely to curb the use of contracts by electronic means; the examination of the legislation requiring such adjustment should be systematic and should cover all the necessary stages and acts of the contractual process, including the filing of the contract; the result of this amendment should be to make contracts concluded electronically workable; the legal effect of electronic signatures is dealt with by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(24); the acknowledgement of receipt by a service provider may take the form of the on-line provision of the service paid for.

(35) This Directive does not affect Member States’ possibility of maintaining or establishing general or specific legal requirements for contracts which can be fulfilled by electronic means, in particular requirements concerning secure electronic signatures.

(36) Member States may maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities, or professions exercising public authority; this possibility also covers contracts which require the involvement of courts, public authorities, or professions exercising public authority in order to have an effect with regard to third parties as well as contracts requiring by law certification or attestation by a notary.

(37) Member States’ obligation to remove obstacles to the use of electronic contracts concerns only obstacles resulting from legal requirements and not practical obstacles resulting from the impossibility of using electronic means in certain cases.

(38) Member States may maintain restrictions for the use of electronic signatures.

(39) The exceptions to the provisions concerning the contracts concluded exclusively by electronic mail or by equivalent individual communications provided for by this Directive, in relation to information to be provided and the placing of orders, should not enable, as a result, the by-passing of those provisions by providers of information society services.

(40) Both existing and emerging disparities in Member States’ legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities. Directive 98/28/EC must provide the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

(41) This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider who deliberately benefits from the exemptions for “mere conduit” and for “caching” when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission, they do not affect the integrity of the information contained in the transmission.

(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of “mere conduit” or “caching” and as a result cannot benefit from the liability exemptions established for these activities; they do not affect the integrity of the information contained in the transmission.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any
infringement, including the removal of illegal information or the disabling of access to it.

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by customers of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

(49) Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

(50) It is important that the proposed directive on the harmonisation of certain aspects of copyright and related rights in the information society and this Directive come into force within a similar time scale with a view to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and relating rights infringements at Community level.

(51) Each Member State should be required, where necessary, to amend any legislation which is liable to hamper the use of schemes for the out-of-court settlement of disputes through electronic channels; the result of this amendment must be to make the functioning of such schemes genuinely and effectively possible in law and in practice, even across borders.

(52) The effective exercise of the freedoms of the internal market are necessary to guarantee victims' effective access to means of settling disputes; damage which may arise in connection with information services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; Member States should examine the need to provide access to judicial procedures by appropriate electronic means.

(53) Directive 98/27/EC, which is applicable to information society services, provides a mechanism relating to actions for an injunction aimed at the protection of the collective interests of consumers; this mechanism will contribute to the free movement of information society services by ensuring a high level of consumer protection.

(54) The sanctions provided for under this Directive are without prejudice to any other sanction or remedy provided under national law; Member States are not obliged to provide criminal sanctions for infringement of national provisions adopted pursuant to this Directive.

(55) This Directive does not affect the law applicable to contractual obligations relating to consumer contracts; accordingly, this Directive cannot have the result of depriving the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence.

(56) As regards the derogation contained in this Directive regarding contractual obligations concerning contracts concluded by consumers, those obligations should be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract.

(57) The Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

(58) This Directive should not apply to services supplied by service providers established in a third country; in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitral) on legal issues.

(59) Despite the global nature of electronic communications, coordination of national regulatory measures at European Union level is necessary in order to avoid fragmentation of the internal market, and for the establishment of an appropriate European regulatory framework; such coordination should also contribute to the establishment of a common and strong negotiating position in international forums.

(60) In order to allow the unhampered development of electronic commerce, the legal framework must be clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.

(61) If a market is actually to operate by electronic means in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible.

(62) Cooperation with third countries should be strengthened and, in the area of electronic commerce, in particular with applicant countries, the developing countries and the European Union's other trading partners.

(63) The adoption of this Directive will not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society; in particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens can have access to the cultural heritage provided in the digital environment.

(64) Electronic communication offers the Member States an excellent means of providing public services in the cultural, educational and linguistic fields.

(65) The Council, in its resolution of 19 January 1999 on the consumer dimension of the information society(25), stressed that the protection of consumers deserved special attention in this field; the Commission will examine the degree to which existing consumer protection rules provide insufficient protection in the context of the information society and will identify, where necessary, the deficiencies of this legislation and those issues which could require additional measures; if need be, the Commission should make specific additional proposals to resolve such deficiencies that will thereby have been identified.

HAY ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Objective and scope
1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.

5. This Directive shall not apply to:
   (a) the field of taxation;
   (b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;
   (c) questions relating to agreements or practices governed by cartel law;
   (d) the following activities of information society services:
      - the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
      - the representation of a client and defence of his interests before the courts,
      - gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Article 2
Definitions
For the purpose of this Directive, the following terms shall bear the following meanings:
(a) "information society services": services within the meaning of Article 1(3) of Directive 98/34/EC as amended by Directive 98/48/EC;
(b) "service provider": any natural or legal person providing an information society service;
(c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;
(d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;
(e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;
(f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:
   - information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,
   - communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;

(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.
(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:
   - the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,
   - the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;
   (ii) The coordinated field does not cover requirements such as:
      - requirements applicable to goods as such,
      - requirements applicable to the delivery of goods,
      - requirements applicable to services not provided by electronic means.

Article 3
Internal market
1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.

2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.

3. Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.

4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:
   (a) the measures shall be:
      (i) necessary for one of the following reasons:
         - public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
         - the protection of public health,
         - public security, including the safeguarding of national security and defence,
         - the protection of consumers, including investors;
      (ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;
      (iii) proportionate to those objectives;
   (b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:
      - asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate;
      - notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.

5. Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible...
time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.

6. Without prejudice to the Member State’s possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.

CHAPTER II

PRINCIPLES

Section 1: Establishment and information requirements

Article 4

Principle excluding prior authorisation

1. Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect.

2. Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services.

Article 5

General information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

   (a) the name of the service provider;
   (b) the geographic address at which the service provider is established;
   (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;
   (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
   (e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;
   (f) as concerns the regulated professions:
      - any professional body or similar institution with which the service provider is registered;
      - the professional title and the Member State where it has been granted;
      - a reference to the applicable professional rules in the Member State of establishment and the means to access them;
      - where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

2. In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously; find out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Article 8

Regulated professions

1. Member States shall ensure that the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.

2. Without prejudice to the autonomy of professional bodies and associations, Member States and the Commission shall encourage professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication in conformity with the rules referred to in paragraph 1.

3. When drawing up proposals for Community initiatives which may become necessary to ensure the proper functioning of the Internal Market with regard to the information referred to in paragraph 2, the Commission shall take due account of codes of conduct applicable at Community level and shall act in close cooperation with the relevant professional associations and bodies.

4. This Directive shall apply in addition to Community Directives concerning access to, and the exercise of, activities of the regulated professions.

Section 3: Contracts concluded by electronic means

Article 9

Treatment of contracts

1. Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

2. Member States may lay down that paragraph 1 shall not apply to all or certain contracts falling into one of the following categories:

   (a) contracts that create or transfer rights in real estate, except for rental rights;
   (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
   (c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
   (d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7

Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Section 2: Commercial communications

Article 6

Information to be provided

1. Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

   (a) the commercial communication shall be clearly identifiable as such;
   (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
   (c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
   (d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

2. Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services.
Article 10
Information to be provided
1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:
   (a) the different technical steps to follow to conclude the contract;
   (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
   (c) the technical means for identifying and correcting input errors prior to the placing of the order;
   (d) the languages offered for the conclusion of the contract.
2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.
3. Contract terms and general conditions provided to the recipient must be made available in a way that allows him to access them.
4. Paragraphs 1 and 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Article 11
Placing of the order
1. Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:
   - the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
   - the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.
2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.
3. Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Article 12
"Mere conduit"
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
   (a) does not initiate the transmission;
   (b) does not select the receiver of the transmission; and
   (c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13
"Caching"
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
   (a) the provider does not modify the information;
   (b) the provider complies with conditions on access to the information;
   (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
   (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
   (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14
Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
   (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15
No general obligation to monitor
1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or
CHAPTER III
IMPLEMENTATION
Article 16
Codes of conduct
1. Member States and the Commission shall encourage:
(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;
(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;
(c) the accessibility of these codes of conduct in the Community languages by electronic means;
(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;
(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.
2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.
Article 17
Out-of-court dispute settlement
1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.
2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.
3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usage or customs relating to electronic commerce.
Article 18
Court actions
1. Member States shall ensure that court actions available under national law concerning information society services’ activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.
2. The Annex to Directive 98/27/EC shall be supplemented as follows:
Article 19
Cooperation
1. Member States shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure that service providers supply them with the requisite information.
2. Member States shall cooperate with other Member States; they shall, to that end, appoint one or several contact points, whose details they shall communicate to the other Member States and to the Commission.
3. Member States shall, as quickly as possible, and in conformity with national law, provide the assistance and information requested by other Member States or by the Commission, including by appropriate electronic means.
4. Member States shall establish contact points which shall be accessible at least by electronic means and from which recipients and service providers may:
(a) obtain general information on contractual rights and obligations as well as on the complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;
(b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.
5. Member States shall encourage the communication to the Commission of any significant administrative or judicial decisions taken in their territory regarding disputes relating to information society services and practices, usages and customs relating to electronic commerce. The Commission shall communicate these decisions to the other Member States.
Article 20
Sanctions
Member States shall determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are enforced. The sanctions they provide for shall be effective, proportionate and dissuasive.
CHAPTER IV
FINAL PROVISIONS
Article 21
Re-examination
1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.
2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, "notice and take down" procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.
Article 22
Transposition
1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 17 January 2002. They shall forthwith inform the Commission thereof.
2. When Member States adopt the measures referred to in paragraph 1, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The methods of making such reference shall be laid down by Member States.
Article 23
Entry into force
This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.
Article 24
Addressees
This Directive is addressed to the Member States.
Done at Luxemburg, 8 June 2000.
For the European Parliament
The President
Relevant Case Law on Directive 2000/31/EC on electronic commerce

Case C-244/06, Dynamic Medien Vertriebs GmbH v Avides Media AG, THE COURT (Third Chamber).

Summary of the Judgment

Free movement of goods – Quantitative restrictions – Measures having equivalent effect

(Art. 28 EC)

National rules which prohibit the sale and transfer by mail order of image storage media which have not been examined and classified by a competent national authority or by a national voluntary self regulatory body for the purposes of protecting young persons and which do not bear a label indicating the age from which they may be viewed, does not constitute a selling arrangement which is capable of hindering, directly or indirectly, actually or potentially intra-Community trade, but a measure having equivalent effect to quantitative restrictions within the meaning of Article 28 EC and is, in principle, incompatible with the obligations arising from that provision.

However, those rules may be compatible with that provision provided that they do not go beyond what is necessary to attain the objective of protecting children pursued by the Member State concerned, as will be the case where the rules do not preclude all forms of marketing of unchecked image storage media but a measure having equivalent effect to quantitative restrictions within the meaning of Article 28 EC and is, in principle, incompatible with the obligations arising from that provision.

For the Council
G. D’Oliveira Martins

N. Fontaine

The President

For the Council

Masaryk University, Faculty of Law

Institute of Law and Technology

54
period or that the decision of refusal cannot be open to challenge before the courts.

(see paras 29, 32, 35, 42, 47-48, operative part)

**Case C-298/07, Bundessverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG,**

Summary of the Judgment


Article 5(1)(c) of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the internal market must be interpreted as meaning that a service provider is required to supply to recipients of the service, before the conclusion of a contract with them, in addition to its electronic mail address, other information which allows the service provider to be contacted rapidly and communicated with in a direct and effective manner. That information does not necessarily have to be a telephone number. That information may be in the form of an electronic enquiry template through which the recipients of the service can contact the service provider via the internet, to whom the service provider replies by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, finds himself without access to the electronic network, requests the latter to provide access to another, non-electronic, means of communication.

(see para. 40, operative part)

**Case C 292/10, G v Cornelius de Visser,**

Ruling:

1. In circumstances such as those in the main proceedings, Article 4(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that it does not preclude the application of Article 5(3) of that regulation to an action for liability arising from the operation of an Internet site against a defendant who is probably a European Union citizen but whose whereabouts are unknown if the court seised of the case does not hold firm evidence to support the conclusion that the defendant is in fact domiciled outside the European Union.

2. European Union law must be interpreted as meaning that it does not preclude the issue of judgment by default against a defendant on whom, given that it is impossible to locate him, the document instituting proceedings has been served by public notice under national law, provided that the court seised of the matter has first satisfied itself that all investigations required by the principles of diligence and good faith have been undertaken to trace the defendant.

3. European Union law must be interpreted as precluding certification as a European Enforcement Order, within the meaning of Regulation (EC) No 805/2004 of the European Parliament and of the Council of 21 April 2004 creating a European Enforcement Order for uncontested claims, of a judgment by default issued against a defendant whose address is unknown.

4. Article 3(1) and (2) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market does not apply to a situation where the place of establishment of the information society services provider is unknown, since application of that provision is subject to identification of the Member State in whose territory the service provider in question is actually established.

**Case C-291/13 Sotiris Papasavvas v O Fileleftheros Dinmosia Etairia Ltd, Takis Kounoufi, Giorgos Sertis,**

Ruling:

1. Article 2(a) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) must be interpreted as meaning that the concept of ‘information society services’, within the meaning of that provision, covers the provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website.

2. In a case such as that at issue in the main proceedings, Directive 2000/31 does not preclude the application of rules of civil liability for defamation.

3. The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge.

4. The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 are capable of applying in the context of proceedings between individuals relating to civil liability for defamation, where the conditions referred to in those articles are satisfied.

5. Articles 12 to 14 of Directive 2000/31 do not allow information society service providers to oppose the bringing of legal proceedings for civil liability against them and, consequently, the adoption of a prohibitory injunction by a national court. The limitations of liability provided for in those articles may be invoked by the provider in accordance with the provisions of national law transposing them or, failing that, for the purpose of an interpretation of that law in conformity with the directive. By contrast, in a case such as that in the main proceedings, Directive 2000/31 cannot, in itself, create obligations on the part of individuals and therefore cannot be relied on against those individuals.

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Article 153(1) and (3)(a) of the Treaty provides that the Community is to contribute to the attainment of a high level of consumer protection by the measures it adopts pursuant to Article 95 thereof.

(2) In accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured. The development of fair commercial practices within the area without internal frontiers is vital for the promotion of the development of cross-border activities.

(3) The laws of the Member States relating to unfair commercial practices show marked differences which can generate appreciable distortions of competition and obstacles to the smooth functioning of the internal market. In the field of advertising, Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising [3] establishes minimum criteria for harmonising legislation on misleading advertising, but does not prevent the Member States from retaining or adopting measures which provide more extensive protection for consumers. As a result, Member States’ provisions on misleading advertising diverge significantly.

(4) These disparities cause uncertainty as to which national rules apply to unfair commercial practices harming consumers’ economic interests and create many barriers affecting business and consumers. These barriers increase the cost to business of exercising internal market freedoms, in particular when businesses wish to engage in cross border marketing, advertising campaigns and sales promotions. Such barriers also make consumers uncertain of their rights and undermine their confidence in the internal market.

(5) In the absence of uniform rules at Community level, obstacles to the free movement of services and goods across borders or the freedom of establishment could be justified in the light of the case-law of the Court of Justice of the European Communities as long as they seek to protect recognised public interest objectives and are proportionate to those objectives. In view of the Community’s objectives, as set out in the provisions of the Treaty and in secondary Community law relating to freedom of movement, and in accordance with the Commission’s policy on commercial communications as indicated in the Communication from the Commission entitled "The follow-up to the Green Paper on Commercial Communications in the Internal Market", such obstacles should be eliminated. These obstacles can only be eliminated by establishing uniform rules at Community level which establish a high level of consumer protection and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market and to meet the requirement of legal certainty.

(6) This Directive therefore approximates the laws of the Member States on unfair commercial practices, including unfair advertising, which directly harm consumers’ economic interests and thereby indirectly harm the economic interests of legitimate competitors. In line with the principle of proportionality, this Directive protects consumers from the consequences of such unfair commercial practices where they are material but recognises that in some cases the impact on consumers may be negligible. It neither covers nor affects the national laws on unfair commercial practices which harm only competitors’ economic interests or which relate to a transaction between traders; taking full account of the principle of subsidiarity, Member States will continue to be able to regulate such practices, in conformity with Community law, if they choose to do so. Nor does this Directive cover or affect the provisions of Directive 84/450/EEC on advertising which misleads business but which is not misleading for consumers and on comparative advertising. Further, this Directive does not affect accepted advertising and marketing practices, such as legitimate product placement, brand differentiation or the offering of incentives which may legitimately affect consumers’ perceptions of products and influence their behaviour without impairing the consumer’s ability to make an informed decision.

(7) This Directive addresses commercial practices directly related to influencing consumers’ transactional decisions in relation to products. It does not address commercial practices carried out primarily for other purposes, including for example commercial communication aimed at investors, such as annual reports and corporate promotional literature. It does not address legal requirements related to taste and decency which vary widely among the Member States. Commercial practices such as, for example, commercial solicitation in the streets, may be undesirable in Member States for cultural reasons. Member States should accordingly be able to continue to ban commercial practices in their territory, in conformity with Community law, for reasons of taste and decency even where such practices do not limit consumers’ freedom of choice. Full account should be taken of the context of the individual case concerned in applying this Directive, in particular the general clauses thereof.

(8) This Directive directly protects consumer economic interests from unfair business-to-consumer commercial practices. Thereby, it also indirectly protects legitimate businesses from their competitors who do not play by the rules in this Directive and thus guarantees fair competition in fields coordinated by it. It is understood that there are other commercial practices which, although not harming consumers, may hurt competitors and business customers. The Commission should carefully examine the need for Community action in the field of unfair competition beyond the remit of this Directive and, if necessary, make a legislative proposal to cover these other aspects of unfair competition.

(9) This Directive is without prejudice to individual actions brought by those who have been harmed by an unfair commercial practice. It is also without prejudice to Community and national rules on contract law, on intellectual property rights, on the health and safety aspects of products, on conditions of establishment and authorisation regimes,
including those rules which, in conformity with Community law, relate to gambling activities, and to Community competition rules and the national provisions implementing them. The Member States will thus be able to retain or introduce restrictions and prohibitions of commercial practices on grounds of the protection of the interests of consumers in their territory wherever the trader is based, for example in relation to alcohol, tobacco or pharmaceuticals. Financial services and immovable property, by reason of their complexity and inherent serious risks, necessitate detailed requirements, including positive obligations on traders. For this reason, in the field of financial services and immovable property, this Directive is without prejudice to the right of Member States to go beyond its provisions to protect the economic interests of consumers. It is not appropriate to regulate here the certification and indication of the standard of fineness of articles of precious metal and the measurement of precious metal in them.

(10) It is necessary to ensure that the relationship between this Directive and existing Community law is coherent, particularly where detailed provisions on unfair commercial practices apply to specific sectors. This Directive therefore amends Directive 84/450/EEC, Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts [4], Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers’ interests [5] and Directive 2002/65/EC of the European Parliament and of the Council of 12 July 2002 concerning the distance marketing of consumer financial services [6]. This Directive accordingly applies only in so far as there are no specific Community law provisions regulating specific aspects of unfair commercial practices, such as information requirements and rules on the way the information is presented to the consumer. It provides protection for consumers where there is no specific sectoral legislation at Community level and prohibits traders from creating a false impression of the nature of products. This is particularly important for complex products with high levels of risk to consumers, such as certain financial services products. This Directive consequently complements the Community acquis, which is applicable to commercial practices harming consumers’ economic interests.

(11) The high level of convergence achieved by the approximation of national provisions through this Directive creates a high common level of consumer protection. This Directive establishes a single general prohibition of those unfair commercial practices distorting consumers’ economic behaviour. It also sets rules on aggressive commercial practices, which are currently not regulated at Community level.

(12) Harmonisation will considerably increase legal certainty for both consumers and business. Both consumers and business will be able to rely on a single regulatory framework based on clearly defined legal concepts regulating all aspects of unfair commercial practices across the EU. The effect will be to eliminate the barriers stemming from the fragmentation of the rules on unfair commercial practices harming consumer economic interests and to enable the internal market to be achieved in this area.

(13) In order to achieve the Community’s objectives through the removal of internal market barriers, it is necessary to replace Member States’ existing, divergent general clauses and legal principles. The single, common general prohibition established by this Directive therefore covers unfair commercial practices distorting consumers’ economic behaviour. In order to support consumer confidence the general prohibition should apply equally to unfair commercial practices which occur outside any contractual relationship between a trader and a consumer or following the conclusion of a contract and during its execution. The general prohibition is elaborated by rules on the two types of commercial practices which are by far the most common, namely misleading commercial practices and aggressive commercial practices.

(14) It is desirable that misleading commercial practices cover those practices, including misleading advertising, which by deceiving the consumer prevent him from making an informed and thus efficient choice. In conformity with the laws and practices of Member States on misleading advertising, this Directive classifies misleading practices into misleading actions and misleading omissions. In respect of omissions, this Directive sets out a limited number of key items of information which the consumer needs to make an informed transactional decision. Such information will not have to be disclosed in all advertising communications by the trader; it only makes an invitation to purchase, which is a concept clearly defined in this Directive. The full harmonisation approach adopted in this Directive does not preclude the Member States from specifying in national law the main characteristics of particular products such as, for example, collectors’ items or electrical goods, the acquisition of which would be material when an invitation to purchase is made. It is not the intention of this Directive to reduce consumer choice by prohibiting the promotion of products which look similar to other products unless this similarity confuses consumers as to the commercial origin of the product and is therefore misleading. This Directive should be without prejudice to existing Community law which expressly affords Member States the choice between several regulatory options for the protection of consumers in the field of commercial practices. In particular, this Directive should be without prejudice to Article 13(3) of Directive 93/13/EEC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [7].

(15) Where Community law sets out information requirements in relation to commercial communication, advertising and marketing that information is considered as material under this Directive. Member States will be able to retain or add information requirements relating to contract law and having contract law consequences where this is allowed by the minimum clauses in the existing Community law instruments. A non-exhaustive list of such information requirements in the acquis is contained in Annex II. Given the full harmonisation introduced by this Directive only the information required in Community law is considered as material for the purpose of Article 7(5) thereof. Where Member States have introduced information requirements over and above what is modified in Community law, on the basis of minimum clauses, the omission of that extra information will not constitute a misleading omission under this Directive. By contrast Member States will be able, when allowed by the minimum clauses in Community law, to maintain or introduce more stringent provisions in conformity with Community law so as to ensure a higher level of protection of consumers’ individual contractual rights.

(16) The provisions on aggressive commercial practices should cover those practices which significantly impair the consumer’s freedom of choice. Those are practices using harassment, coercion, including the use of physical force, and undue influence.

(17) It is desirable that those commercial practices which are in all circumstances unfair be identified to provide greater legal certainty. Annex I therefore contains the full list of all such practices. These are the only commercial practices which can be deemed to be general clauses and legal principles. The single, common general prohibition established by this Directive therefore covers unfair commercial practices distorting consumers’ economic behaviour. In order to support consumer confidence the general prohibition should apply equally to unfair commercial practices which occur outside any contractual relationship between a trader and a consumer or following the conclusion of a contract and during its execution. The general prohibition is elaborated by rules on the two types of commercial practices which are by far the most common, namely misleading commercial practices and aggressive commercial practices.
interpreted by the Court of Justice, but also contains provisions aimed at preventing the exploitation of consumers whose characteristics make them particularly vulnerable to unfair commercial practices. Where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is not acceptable that the impact of the commercial practice be assessed from the perspective of the average member of that group. It is therefore appropriate to include in the list of practices which are in all circumstances unfair a provision which, without imposing an outright ban on advertising directed at children, protect them from direct exhortations to purchase. The average consumer test is not a statistical test. National courts and authorities will have to exercise their own faculty of judgement, having regard to the case-law of the Court of Justice, to determine the typical reaction of the average consumer in a given case. (19) Where certain characteristics such as age, physical or mental infirmity or credulity make consumers particularly susceptible to a commercial practice or to the underlying product and the economic behaviour only of such consumers is likely to be distorted by the practice in a way that the trader can reasonably foresee, it is appropriate to ensure that they are adequately protected by assessing the practice from the perspective of the average member of that group. (20) It is appropriate to provide a role for codes of conduct, which enable traders to apply the principles of this Directive effectively in specific economic fields. In sectors where there are specific mandatory requirements regulating the behaviour of traders, it is appropriate that these will also provide evidence as to the requirements of professional diligence in that sector. The control exercised by code owners at national or Community level to eliminate unfair commercial practices may avoid the need for recourse to administrative or judicial action and should therefore be encouraged. With the aim of pursuing a high level of consumer protection, consumers’ organisations could be informed and involved in the drafting of codes of conduct. (21) Persons or organisations regarded under national law as having a legitimate interest in the matter must have legal remedies for initiating proceedings against unfair commercial practices, either before a court or before an administrative authority which is competent to decide upon complaints or to initiate appropriate legal proceedings. While it is for national law to determine the burden of proof, it is appropriate to enable courts and administrative authorities to require traders to produce evidence as to the accuracy of factual claims they have made. (22) It is necessary that Member States lay down penalties for infringements of the provisions of this Directive and they must ensure that these are enforced. The penalties must be effective, proportionate and dissuasive. (23) Since the objectives of this Directive, namely to eliminate the barriers to the functioning of the internal market represented by national laws on unfair commercial practices and to provide a high common level of consumer protection, by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to eliminate the internal market barriers and achieve a high common level of consumer protection. (24) It is appropriate to review this Directive to ensure that barriers to the internal market have been addressed and a high level of consumer protection achieved. The review could lead to a Commission proposal to amend this Directive, which may include a limited extension to the derogation in Article 3(5), and/or amendments to other consumer protection legislation reflecting the Commission’s Consumer Policy Strategy commitment to review the existing acquis in order to achieve a high, common level of consumer protection. (25) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, and H A V E A D O P T E D T H I S D I R E C T I V E: CHAPTER 1 GENERAL PROVISIONS Article 1 Purpose The purpose of this Directive is to contribute to the proper functioning of the internal market and achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers’ economic interests. Article 2 Definitions For the purposes of this Directive: (a) "consumer" means any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession; (b) "trader" means any natural or legal person who, in commercial practices covered by this Directive, is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader; (c) "product" means any goods or service including immovable property, rights and obligations; (d) "business-to-consumer commercial practices" (hereinafter also referred to as commercial practices) means any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers; (e) "to materially distort the economic behaviour of consumers" means using a commercial practice to appreciably impair the consumer’s ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise; (f) "code of conduct" means an agreement or set of rules not imposed by law, regulation or administrative provision of a Member State which defines the behaviour of traders who undertake to be bound by the code in relation to one or more particular commercial practices or business sectors; (g) "code owner" means any entity, including a trader or group of traders, which is responsible for the formulation and revision of a code of conduct and/or for monitoring compliance with the code by those who have undertaken to be bound by it; (h) "professional diligence" means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader’s field of activity; (i) "invitation to purchase" means a commercial communication which indicates characteristics of the product and the price in a way appropriate to the means of the commercial communication used and thereby enables the consumer to make a purchase; (j) "undue influence" means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer’s ability to make an informed decision; (k) "transactional decision" means any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting; (l) "regulated profession" means a professional activity or a group of professional activities, access to which or the pursuit of which, or one of the modes of pursuing which, is conditional, directly or indirectly, upon possession of specific...
professional qualifications, pursuant to laws, regulations or administrative provisions.

Article 3
Scope
1. This Directive shall apply to unfair business-to-consumer commercial practices, as laid down in Article 5, before, during and after a commercial transaction in relation to a product.
2. This Directive is without prejudice to contract law and, in particular, to the rules on the validity, formation or effect of a contract.
3. This Directive is without prejudice to Community or national rules relating to the health and safety aspects of products.
4. In the case of conflict between the provisions of this Directive and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects.
5. For a period of six years from 12 June 2007, Member States shall be able to continue to apply national provisions within the field approximated by this Directive which are more restrictive or prescriptive than this Directive and which implement directives containing minimum harmonisation clauses. These measures must be essential to ensure that consumers are adequately protected against unfair commercial practices and must be proportionate to the attainment of this objective. The review referred to in Article 18 may, if considered appropriate, include a proposal to prolong this derogation for a further limited period.
6. Member States shall notify the Commission without delay of any national provisions applied on the basis of paragraph 5.
7. This Directive is without prejudice to the rules determining the jurisdiction of the courts.
8. This Directive is without prejudice to any conditions of establishment or of authorisation regimes, or to the deontological codes of conduct or other specific rules governing regulated professions in order to uphold high standards of integrity on the part of the professional, which Member States may, in conformity with Community law, impose on professionals.
9. In relation to "financial services", as defined in Directive 2002/65/EC, and immovable property, Member States may impose requirements which are more restrictive or prescriptive than this Directive in the field which it approximates.
10. This Directive shall not apply to the application of the laws, regulations and administrative provisions of Member States relating to the certification and indication of the standard of fineness of articles of precious metal.

Article 4
Internal market
Member States shall neither restrict the freedom to provide services nor restrict the free movement of goods for reasons falling within the field approximated by this Directive.

CHAPTER 2
UNFAIR COMMERCIAL PRACTICES

Article 5
Prohibition of unfair commercial practices
1. Unfair commercial practices shall be prohibited.
2. A commercial practice shall be unfair if:
   (a) it is contrary to the requirements of professional diligence, and
   (b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.
3. Commercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way in which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.
4. In particular, commercial practices shall be unfair which:
   (a) are misleading as set out in Articles 6 and 7,
   or
   (b) are aggressive as set out in Articles 8 and 9.
5. Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. The same single list shall apply in all Member States and may only be modified by revision of this Directive.

Section 1
Misleading commercial practices

Article 6
Misleading actions
1. A commercial practice shall be regarded as misleading if it contains false information and is therefore untrue or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causing or is likely to cause him to take a transactional decision that he would not have taken otherwise:
   (a) the existence or nature of the product;
   (b) the main characteristics of the product, such as its availability, benefits, risks, execution, composition, accessories, after-sale customer assistance and complaint handling, method and date of manufacture or provision, delivery, fitness for purpose, usage, quantity, specification, geographical or commercial origin or the results to be expected from its use, or the results and material features of tests or checks carried out on the product;
   (c) the extent of the trader's commitments, the motives for the commercial practice and the nature of the sales process, any statement or symbol in relation to direct or indirect sponsorship or approval of the trader or the product;
   (d) the price or the manner in which the price is calculated, or the existence of a specific price advantage;
   (e) the need for a service, part, replacement or repair;
   (f) the nature, attributes and rights of the trader or his agent, such as his identity and assets, his qualifications, status, approval, affiliation or connection and ownership of industrial, commercial or intellectual property rights or his awards and distinctions;
   (g) the consumer's rights, including the right to replacement or reimbursement under Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [8], or the risks he may face.
2. A commercial practice shall also be regarded as misleading if, in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise, and it involves:
   (a) any marketing of a product, including comparative advertising, which creates confusion with any products, trademarks, trade names or other distinguishing marks of a competitor;
   (b) non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound, where:
      (i) the commitment is not aspirational but is firm and is capable of being verified,
      and
      (ii) the trader indicates in a commercial practice that he is bound by the code.
Article 7
Misleading omissions
1. A commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.
2. It shall also be regarded as a misleading omission when, taking account of the matters described in paragraph 1, a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.
3. Where the medium used to communicate the commercial practice imposes limitations of space or time, these limitations and any measures taken by the trader to make the information available to consumers by other means shall be taken into account in deciding whether information has been omitted.
4. In the case of an invitation to purchase, the following information shall be regarded as material, if not already apparent from the context: (a) the main characteristics of the product, to an extent appropriate to the medium and the product; (b) the geographical address and the identity of the trader, such as his trading name and, where applicable, the geographical address and the identity of the trader on whose behalf he is acting; (c) the price inclusive of taxes, or where the nature of the product means that the price cannot reasonably be calculated in advance, the manner in which the price is calculated, as well as, where appropriate, all additional freight, delivery or postal charges or, where these charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable; (d) the arrangements for payment, delivery, performance and the complaint handling policy, if they depart from the requirements of professional diligence; (e) for products and transactions involving a right of withdrawal or cancellation, the existence of such a right.
5. Information requirements established by Community law in relation to commercial communication including advertising or marketing, a non-exhaustive list of which is contained in Annex II, shall be regarded as material.

Section 2
Aggressive commercial practices
Article 8
Aggressive commercial practices
A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer’s freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.

Article 9
Use of harassment, coercion and undue influence
In determining whether a commercial practice uses harassment, coercion, including the use of physical force, or undue influence, account shall be taken of: (a) its timing, location, nature or persistence; (b) the use of threatening or abusive language or behaviour; (c) the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer’s judgement, of which the trader is aware, to influence the consumer’s decision with regard to the product; (d) any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader; (e) any threat to take any action that cannot legally be taken.

CHAPTER 3
CODES OF CONDUCT
Article 10
Codes of conduct
This Directive does not exclude the control, which Member States may encourage, of unfair commercial practices by code owners and recourse to such bodies by the persons or organisations referred to in Article 11 if proceedings before such bodies are in addition to the court or administrative proceedings referred to in that Article.
Recourse to such control bodies shall never be deemed the equivalent of foregoing a means of judicial or administrative recourse as provided for in Article 11.

CHAPTER 4
FINAL PROVISIONS
Article 11
Enforcement
1. Member States shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provisions of this Directive in the interest of consumers.
Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commercial practices, including competitors, may: (a) take legal action against such unfair commercial practices; and/or (b) bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.
It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 10. These facilities shall be available regardless of whether the consumers affected are in the territory of the Member State where the trader is located or in another Member State.
It shall be for each Member State to decide: (a) whether these legal facilities may be directed separately or jointly against a number of traders from the same economic sector; and (b) whether these legal facilities may be directed against a code owner where the relevant code promotes non-compliance with legal requirements.
2. Under the legal provisions referred to in paragraph 1, Member States shall confer upon the courts or administrative authorities powers enabling them, in cases where they deem such measures to be necessary taking into account all the interests involved and in particular the public interest: (a) to order the cessation of, or to institute appropriate legal proceedings for an order for the cessation of, unfair commercial practices; or (b) if the unfair commercial practice has not yet been carried out but is imminent, to order the prohibition of the practice, or to institute appropriate legal proceedings for an order for the prohibition of the practice, even without proof of actual loss or damage or of intention or negligence on the part of the trader.
Member States shall also make provision for the measures referred to in the first subparagraph to be taken under an accelerated procedure: - either with interim effect, or - with definitive effect, on the understanding that it is for each Member State to decide which of the two options to select.
Furthermore, Member States may confer upon the courts or administrative authorities powers enabling them, with a view to eliminating the continuing effects of unfair commercial practices the cessation of which has been ordered by a final decision:
(a) to require publication of that decision in full or in part and in such form as they deem adequate;
(b) to require in addition the publication of a corrective statement.
3. The administrative authorities referred to in paragraph 1 must:
(a) be composed so as not to cast doubt on their impartiality;
(b) have adequate powers, where they decide on complaints, to monitor and enforce the observance of their decisions effectively;
(c) normally give reasons for their decisions.
Where the powers referred to in paragraph 2 are exercised exclusively by an administrative authority, reasons for its decisions shall always be given. Furthermore, in this case, provision must be made for procedures whereby improper or unreasonable exercise of its powers by the administrative authority or improper or unreasonable failure to exercise the said powers can be the subject of judicial review.

Article 12
Courts and administrative authorities: substantiation of claims
Member States shall confer upon the courts or administrative authorities powers enabling them in the civil or administrative proceedings provided for in Article 11:
(a) to require the trader to furnish evidence as to the accuracy of factual claims in relation to a commercial practice if, taking into account the legitimate interest of the trader and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case;
and
(b) to consider factual claims as inaccurate if the evidence demanded in accordance with (a) is not furnished or is deemed insufficient by the court or administrative authority.

Article 13
Penalties
Member States shall lay down penalties for infringements of national provisions adopted in application of this Directive and shall take all necessary measures to ensure that these are enforced. These penalties must be effective, proportionate and dissuasive.

Article 14
Amendments to Directive 84/450/EEC
Directive 84/450/EEC is hereby amended as follows:
1. Article 1 shall be replaced by the following:
"Article 1
The purpose of this Directive is to protect traders against misleading advertising and the unfair consequences thereof and to lay down the conditions under which comparative advertising is permitted."

2. in Article 2:
- point 3 shall be replaced by the following:
"3. "trader" means any natural or legal person who is acting for purposes relating to his trade, craft, business or profession and any one acting in the name of or on behalf of a trader."
- the following point shall be added:
"4. "code owner" means any entity, including a trader or group of traders, which is responsible for the formulation and revision of a code of conduct and/or for monitoring compliance with the code by those who have undertaken to be bound by it."

3. Article 3a shall be replaced by the following:
"Article 3a
1. Comparative advertising shall, as far as the comparison is concerned, be permitted when the following conditions are met:
(a) it is not misleading within the meaning of Articles 2(2), 3 and 7(1) of this Directive or Articles 6 and 7 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [ ];
(b) it compares goods or services meeting the same needs or intended for the same purpose;
(c) it objectively compares one or more material, relevant, verifiable and representative features of those goods and services, which may include price;
(d) it does not discredit or denigrate the trade marks, trade names, other distinguishing marks of a competitor or of the designation of origin of competing products;
(e) for products with designation of origin, it relates in each case to products with the same designation;
(f) it does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;
(g) it does not present goods or services as imitations or replicas of goods or services bearing a protected trade mark or trade name;
(h) it does not create confusion among traders, between the advertiser and a competitor or between the advertiser’s trade marks, trade names, other distinguishing marks, goods or services and those of a competitor.
4. Article 4(1) shall be replaced by the following:
"1. Member States shall ensure that adequate and effective means exist to combat misleading advertising in order to enforce compliance with the provisions on comparative advertising in the interest of traders and competitors. Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating misleading advertising or regulating comparative advertising may:
(a) take legal action against such advertising;
or
(b) bring such advertising before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.
It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 5. It shall be for each Member State to decide:
(a) whether these legal facilities may be directed separately or jointly against a number of traders from the same economic sector;
and
(b) whether these legal facilities may be directed against a code owner where the relevant code promotes non-compliance with legal requirements.
"
5. Article 7(1) shall be replaced by the following:
"1. This Directive shall not preclude Member States from retaining or adopting provisions with a view to ensuring more extensive protection, with regard to misleading advertising, for traders and competitors."

Article 15
Amendments to Directives 97/7/EC and 2002/65/EC
1. Article 9 of Directive 97/7/EC shall be replaced by the following:
"Article 9
Inertia selling
Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [ ], Member States shall take the measures necessary to exempt the consumer from the provision of any consideration in cases of unsolicited supply, the absence of a response not constituting consent."
Article 9 of Directive 2002/65/EC shall be replaced by the following:

"Article 9
Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [1] and without prejudice to the provisions of Member States’ legislation on the tacit renewal of distance contracts, when such rules permit tacit renewal, Member States shall take measures to exempt the consumer from any obligation in the event of unsolicited supplies, the absence of a reply not constituting consent.

Article 16
1. In the Annex to Directive 98/27/EC, point 1 shall be replaced by the following:


2. In the Annex to Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of the consumer protection law (the Regulation on consumer protection cooperation) [12] the following point shall be added:


Article 17
Information
Member States shall take appropriate measures to inform consumers of the national law transposing this Directive and shall, where appropriate, encourage traders and code owners to inform consumers of their codes of conduct.

Article 18
Review
1. By 12 June 2011 the Commission shall submit to the European Parliament and the Council a comprehensive report on the application of this Directive, in particular of Articles 3(9) and 4 and Annex I, on the scope for further harmonisation and simplification of Community law relating to consumer protection, and, having regard to Article 3(5), on any measures that need to be taken at Community level to ensure that appropriate levels of consumer protection are maintained. The report shall be accompanied, if necessary, by a proposal to revise this Directive or other relevant parts of Community law.

2. The European Parliament and the Council shall endeavour to act, in accordance with the Treaty, within two years of the presentation by the Commission of any proposal submitted under paragraph 1.

Article 19
Transposition
Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by 12 June 2007. They shall forthwith inform the Commission thereof and inform the Commission of any subsequent amendments without delay.

They shall apply those measures by 12 December 2007. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 20
Entry into force
This Directive shall enter into force on the day following its publication in the Official Journal of the European Union.

Article 21
Addressess
This Directive is addressed to the Member States.
9. Stating or otherwise creating the impression that a product can legally be sold when it cannot.
10. Presenting rights given to consumers in law as a distinctive feature of the trader’s offer.
11. Using editorial content in the media to promote a product where the trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer (advertorial). This is without prejudice to Council Directive 89/552/EEC [1].
12. Making a materially inaccurate claim concerning the nature and extent of the risk to the personal security of the consumer or his family if the consumer does not purchase the product.
13. Promoting a product similar to a product made by a particular manufacturer in such a manner as deliberately to mislead the consumer into believing that the product is made by that same manufacturer when it is not.
14. Establishing, operating or promoting a pyramid promotional scheme where a consumer gives consideration for the opportunity to receive compensation that is derived primarily from the introduction of other consumers into the scheme rather than from the sale or consumption of products.
15. Claiming that the trader is about to cease trading or move premises when he is not.
16. Claiming that products are able to facilitate winning in games of chance.
17. Falsely claiming that a product is able to cure illnesses, dysfunctions or malformations.
18. Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions.
19. Claiming in a commercial practice to offer a competition or prize promotion without awarding the prizes described or a reasonable equivalent.
20. Describing a product as “gratuit”, “free”, “without charge” or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.
21. Including in marketing material an invoice or similar document seeking payment which gives the consumer the impression that he has already ordered the marketed product when he has not.
22. Falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer.
23. Creating the false impression that after-sales service in relation to a product is available in a Member State other than the one in which the product is sold.
Aggressive commercial practices
24. Creating the impression that the consumer cannot leave the premises until a contract is formed.
25. Conducting personal visits to the consumer’s home ignoring the consumer’s request to leave or not to return except in circumstances and to the extent justified, under national law, to enforce a contractual obligation.
26. Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to Article 10 of Directive 97/7/EC and Directives 95/46/EC [2] and 2002/58/EC.
27. Requiring a consumer who wishes to claim on an insurance policy to produce documents which could not reasonably be considered relevant as to whether the claim was valid, or failing systematically to respond to pertinent correspondence, in order to dissuade a consumer from exercising his contractual rights.
28. Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them. This provision is without prejudice to Article 16 of Directive 89/552/EEC on television broadcasting.
29. Demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer except where the product is a substitute supplied in conformity with Article 7(3) of Directive 97/7/EC (inertia selling).
30. Explicitly informing a consumer that if he does not buy the product or service, the trader’s job or livelihood will be in jeopardy.
31. Creating the false impression that the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either: - there is no prize or other equivalent benefit, or - taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.

20050511

ANNEX II

COMMUNITY LAW PROVISIONS SETTING OUT RULES FOR ADVERTISING AND COMMERCIAL COMMUNICATION

Articles 4 and 5 of Directive 97/7/EC


Articles 3 and 4 of Directive 2002/65/EC


20050511


Articles 5, 7 and 8 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading [12]


Relevant Case Law on Unfair Commercial Practices Directive

Case C-122/10, Konsumentombudsmannen v Ving Sverige AB

(Reference for a preliminary ruling – Directive 2005/29/EC – Articles 2(i) and 7(4) – Commercial communication published in a newspaper – Meaning of invitation to purchase – Entry-level price – Information which an invitation to purchase has to contain).

Ruling:


2. Article 2(i) of Directive 2005/29 must be interpreted as meaning that the requirement relating to the indication of the price of the product may be met if the commercial communication contains an entry-level price, that is to say the lowest price for which the advertised product or category of products can be bought, while the advertised product or category of products are available in other versions or with other content at prices which are not indicated. It is for the national court to ascertain, on the basis of the nature and characteristics of the product and the commercial medium of communication used, whether the reference to an entry-level price enables the consumer to take a transactional decision.

3. Article 2(i) of Directive 2005/29 must be interpreted as meaning that a verbal or visual reference to the product makes it possible to meet the requirement relating to the indication of the product’s characteristics, and that includes a situation where such a verbal or visual reference is used to designate a product which is offered in many versions. It is for the national court to ascertain, on a case-by-case basis, taking into account the nature and characteristics of the product and the medium of communication used, whether the consumer has sufficient information to identify and distinguish the product for the purpose of taking a transactional decision.

4. Article 7(4)(a) of Directive 2005/29 must be interpreted as meaning that it may be sufficient for only certain of a product’s main characteristics to be given and for the trader to refer in addition to its website, on the condition that on that site there is essential information on the product’s main characteristics, price and other terms in accordance with the requirements in Article 7 of that directive. It is for the national court to assess, on a case-by-case basis, taking into consideration the context of the invitation to purchase, the medium of communication used and the nature and characteristics of the product, whether a reference only to certain main characteristics of the product enables the consumer to take an informed transactional decision.

5. Article 7(4)(c) of Directive 2005/29 must be interpreted as meaning that a reference only to an entry-level price in an invitation to purchase cannot be regarded, in itself, as constituting a misleading omission. It is for the national court to ascertain whether a reference to an entry-level price is sufficient for the requirements concerning the reference to a price, such as those set out in that provision, to be considered to be met. That court will have to ascertain, inter alia, whether the omission of the detailed rules for calculating the final price prevents the consumer from taking an informed transactional decision and, consequently, leads him to take a transactional decision which he would not otherwise have taken. It is also for the national court to take into consideration the limitations forming an integral part of the medium of communication used; the nature and the characteristics of the product and the other measures that the trader has actually taken to make the information available to consumers.

Case C-657/11, Belgian Electronic Sorting Technology NV v Bert Peeelaers, Visys NV,

(Directives 84/450/EEC and 2006/114/EC – Misleading and comparative advertising – Definition of ‘advertising’ – Registration and use of a domain name – Use of metatags in a website’s metadata)

the Council of 12 December 2006 concerning misleading and comparative advertising, must be interpreted as meaning that the term 'advertising', as defined by those provisions, covers, in a situation such as that at issue in the main proceedings, the use of a domain name and that of metatags in a website’s metadata. By contrast, the registration of a domain name, as such, is not encompassed by that term.
II. Competition Law

Treaty on the Functioning of the European Union
(101 – 109)

CHAPTER 1: RULES ON COMPETITION

SECTION 1: RULES APPLYING TO UNDERTAKINGS

Article 101 (ex Article 81 TEC)
1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:
(a) directly or indirectly fix purchase or selling prices or any other trading conditions;
(b) limit or control production, markets, technical development, or investment;
(c) share markets or sources of supply;
(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.
2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.
3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:
- any agreement or category of agreements between undertakings;
- any decision or category of decisions by associations of undertakings;
- any concerted practice or category of concerted practices, which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:
(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;
(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Article 102 (ex Article 82 TEC)
Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in:
(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

Article 103 (ex Article 83 TEC)
1. The appropriate regulations or directives to give effect to the principles set out in Articles 101 and 102 shall be laid down by the Council, on a proposal from the Commission and after consulting the European Parliament.
2. The regulations or directives referred to in paragraph 1 shall be designed in particular:
(a) to ensure compliance with the prohibitions laid down in Article 101(1) and in Article 102 by making provision for fines and periodic penalty payments;
(b) to lay down detailed rules for the application of Article 101(3), taking into account the need to ensure effective supervision on the one hand, and to simplify administration to the greatest possible extent on the other;
(c) to define, if need be, in the various branches of the economy, the scope of the provisions of Articles 101 and 102;
(d) to define the respective functions of the Commission and of the Court of Justice of the European Union in applying the provisions laid down in this paragraph;
(e) to determine the relationship between national laws and the provisions contained in this Section or adopted pursuant to this Article.

Article 104 (ex Article 84 TEC)
Until the entry into force of the provisions adopted in pursuance of Article 103, the authorities in Member States shall rule on the admissibility of agreements, decisions and concerted practices and on abuse of a dominant position in the internal market in accordance with the law of their country and with the provisions of Article 101, in particular paragraph 3, and of Article 102.

Article 105 (ex Article 85 TEC)
1. Without prejudice to Article 104, the Commission shall ensure the application of the principles laid down in Articles 101 and 102. On application by a Member State or on its own initiative, and in cooperation with the competent authorities in the Member States, which shall give it their assistance, the Commission shall investigate cases of suspected infringement of these principles. If it finds that there has been an infringement, it shall propose appropriate measures to bring it to an end.
2. If the infringement is not brought to an end, the Commission shall record such infringement of the principles in a reasoned decision. The Commission may publish its decision and authorise Member States to take the measures, the conditions and details of which it shall determine, needed to remedy the situation.
3. The Commission may adopt regulations relating to the categories of agreement in respect of which the Council has
adopted a regulation or a directive pursuant to Article 103(2)(b).

**Article 106** (ex Article 86 TEC)

1. In the case of public undertakings and undertakings to which Member States grant special or exclusive rights, Member States shall neither enact nor maintain in force any measure contrary to the rules contained in the Treaties, in particular to those rules provided for in Article 18 and Articles 107 to 109.

2. Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in the Treaties, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them. The development of trade must not be affected to such an extent as would be contrary to the interests of the Union.

3. The Commission shall ensure the application of the provisions of this Article and shall, where necessary, address appropriate directives or decisions to Member States.

**SECTION 2: AIDS GRANTED BY STATES**

**Article 107** (ex Article 87 TEC)

1. Save as otherwise provided in the Treaties, any aid granted by a Member State or through State resources in any form whatsoever which distorts or threatens to distort competition by favouring certain undertakings or the production of certain goods shall, in so far as it affects trade between Member States, be incompatible with the internal market.

2. The following shall be compatible with the internal market:
   (a) aid having a social character, granted to individual consumers, provided that such aid is granted without discrimination related to the origin of the products concerned;
   (b) aid to make good the damage caused by natural disasters or exceptional occurrences;
   (c) aid granted to the economy of certain areas of the Federal Republic of Germany affected by the division of Germany, in so far as such aid is required in order to compensate for the economic disadvantages caused by that division. Five years after the entry into force of the Treaty of Lisbon, the Council, acting on a proposal from the Commission, may adopt a decision repealing this point.

3. The following may be considered to be compatible with the internal market:
   (a) aid to promote the economic development of areas where the standard of living is abnormally low or where there is serious underemployment, and of the regions referred to in Article 349, in view of their structural, economic and social situation;
   (b) aid to promote the execution of an important project of common European interest or to remedy a serious disturbance in the economy of a Member State;
   (c) aid to facilitate the development of certain economic activities or of certain economic areas, where such aid does not adversely affect trading conditions to an extent contrary to the common interest;
   (d) aid to promote culture and heritage conservation where such aid does not affect trading conditions and competition in the Union to an extent that is contrary to the common interest;
   (e) such other categories of aid as may be specified by decision of the Council on a proposal from the Commission.

**Article 108** (ex Article 88 TEC)

1. The Commission shall, in cooperation with Member States, keep under constant review all systems of aid existing in those States. It shall propose to the latter any appropriate measures required by the progressive development or by the functioning of the internal market.

2. If, after giving notice to the parties concerned to submit their comments, the Commission finds that aid granted by a State or through State resources is not compatible with the internal market having regard to Article 107, or that such aid is being misused, it shall decide that the State concerned shall abolish or alter such aid within a period of time to be determined by the Commission.

If the State concerned does not comply with this decision within the prescribed time, the Commission or any other interested State may, derogation from the provisions of Articles 258 and 259, refer the matter to the Court of Justice of the European Union direct.

On application by a Member State, the Council may, acting unanimously, decide that aid which that State is granting or intends to grant shall be considered to be compatible with the internal market, in derogation from the provisions of Article 107 or from the regulations provided for in Article 109, if such a decision is justified by exceptional circumstances. If, as regards the aid in question, the Commission has already initiated the procedure provided for in the first subparagraph of this paragraph, the fact that the State concerned has made its application to the Council shall have the effect of suspending that procedure until the Council has made its attitude known.

If, however, the Council has not made its attitude known within three months of the said application being made, the Commission shall give its decision on the case.

3. The Commission shall be informed, in sufficient time to enable it to submit its comments, of any plans to grant or alter aid. If it considers that such a plan is not compatible with the internal market having regard to Article 107, it shall without delay initiate the procedure provided for in paragraph 2.

2. The Member State concerned shall not put its proposed measures into effect until this procedure has resulted in a final decision.

4. The Commission may adopt regulations relating to the categories of State aid that the Council has, pursuant to Article 109, determined may be exempted from the procedure provided for by paragraph 3 of this Article.

**Article 109** (ex Article 89 TEC)

The Council, on a proposal from the Commission and after consulting the European Parliament, may make any appropriate regulations for the application of Articles 107 and 108 and may in particular determine the conditions in which Article 108(3) shall apply and the categories of aid exempted from this procedure.
Relevant case-law to the Treaty on the Functioning of the EU
Art 101-102

Case C-52/07- Kanal 5 Ltd and TV 4 AB v Föreningen Svenska Tonsättare Internationella Musikbyrå (STIM) upa

Summary of the Judgment
1. Competition – Dominant position – Copyright management organisation having a de facto monopoly – Collection of royalties corresponding to part of the revenue of commercial television channels which is proportionate overall to the quantity of musical works broadcast in the absence of other methods enabling the use of those works and the audience to be measured more precisely

(Art. 82 EC)

2. Competition – Dominant position – Copyright management organisation having a de facto monopoly – Collection of royalties calculated in a different manner according to whether the companies are commercial companies or public service undertakings

(Art. 82 EC)

1. Article 82 EC must be interpreted as meaning that a copyright management organisation with a dominant position on a substantial part of the common market does not abuse that position where, with respect to remuneration paid for the television broadcast of musical works protected by copyright, it applies to commercial television channels a remuneration model according to which the amount of the royalties corresponds partly to the revenue of those channels, provided that part is proportionate overall to the quantity of musical works protected by copyright actually broadcast or likely to be broadcast, unless another method enables the use of those works and the audience to be identified more precisely without however resulting in a disproportionate increase in the costs incurred for the management of contracts and the supervision of the use of those works.

(see para. 41, operative part 1)

2. Article 82 EC must be interpreted as meaning that, by calculating the royalties with respect to remuneration paid for the broadcast of musical works protected by copyright in a different manner according to whether the companies concerned are commercial companies or public service undertakings, a copyright management organisation is likely to exploit in an abusive manner its dominant position within the meaning of that article if it applies with respect to those companies dissimilar conditions to equivalent services and if it places them as a result at a competitive disadvantage, unless such a practice may be objectively justified.

As regards the examination as to whether such a practice exists account must be taken, where appropriate, of the fact that, unlike commercial television companies, public service undertakings do not have either advertising revenue or revenue relating to subscription contracts and of the fact that the royalties paid by public service undertakings are collected without taking account of the quantity of musical works protected by copyright actually broadcast. Furthermore, it must also be ascertained whether commercial television companies are competitors of public service undertakings on the same market.

As regards the examination of any objective justification, such justification may arise, in particular, from the task and method of financing of public service undertakings.

(see paras 44-48, operative part 2)

Case C-425/07 P AEPI Elliniki Etaireia pros Prostasian tis Pnevmatikis Idioktitias AE v Commission of the European Communities

1 Summary of the Judgment
1. Competition – Administrative procedure – Examination of complaints – Assessment of the Community interest in investigating a case

(Art 81 EC and 82 EC)

2. Competition – Agreements, decisions and concerted practices – Effect on trade between Member States – Meaning

(Art 81 EC and 82 EC)

3. Appeals – Grounds – Grounds of a judgment vitiated by a confusion between two legal concepts – Operative part well founded on other legal grounds – Rejection

1. The Commission is responsible for defining and implementing Community competition policy and for that purpose has a discretion as to how it deals with complaints lodged with it. When the Commission determines the order of priority for dealing with the complaints brought before it, it may legitimately refer to the Community interest. In this context, it is required to assess in each case how serious the alleged interferences with competition are and how persistent their consequences are. That obligation means in particular that it must take into account the duration and extent of the infringements complained of and their effect on the competition situation in the European Community.

Consequently, in a situation where intra-Community trade is found to be affected, a complaint relating to infringement of Articles 81 EC and 82 EC will be investigated by the Commission rather than by the national competition authorities if there is sufficient Community interest. That may inter alia apply where the infringement complained of is capable of giving rise to serious impediments to the proper functioning of the common market.

(see paras 31, 53-54)

2. The concepts of, first, an effect on intra-Community trade and, secondly, of serious impediments to the proper functioning of the common market are two separate concepts.

The effect on trade between Member States serves as a criterion to define the scope of Community competition law, in particular Articles 81 EC and 82 EC, as against that of national competition law. If it is established that the alleged infringement is not capable of affecting intra-Community trade or of affecting it only in an insignificant manner, then Community competition law, and more specifically Articles 81
EC and 82 EC, do not apply. Furthermore, if an agreement between undertakings is to be capable of affecting trade between Member States, it must be possible to foresee with a sufficient degree of probability, on the basis of a set of objective factors of law or of fact, that it has an influence, direct or indirect, actual or potential, on the pattern of trade between Member States in a manner which might harm the attainment of the objectives of a single market between Member States.

As for the concept of serious impediments to the proper functioning of the common market, it may constitute one of the criteria for evaluating whether there is sufficient Community interest to necessitate the investigation of a complaint by the Commission.

An effect on intra-Community trade does not in itself give rise to serious impediments to the proper functioning of the common market.

(see paras 48-52)

3. A confusion of concepts by the Court of First Instance in a judgment under appeal is not capable of giving rise to the annulling of that judgment if the operative part of the judgment is shown to be well founded for other legal reasons.

(see para. 55)

**Case C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG**

1. Where the national courts give a ruling on agreements or practices which may subsequently be the subject of a decision by the Commission, they must avoid taking decisions which conflict with those taken or envisaged by the Commission in the implementation of Articles 81 and 82 EC.

(see para. 19)

2. In the assessment of the abusive character of a dominant position, in order to determine whether a product or service is indispensable for enabling an undertaking to carry on business in a particular market, it must be determined whether there are products or services which constitute alternative solutions, even if they are less advantageous, and whether there are technical, legal or economic obstacles capable of making it impossible or at least unreasonably difficult for any undertaking seeking to operate in the market to create, possibly in cooperation with other operators, alternative products or services. In order to accept the existence of economic obstacles, it must be established, at the very least, that the creation of those products or services is not economically viable for production on a scale comparable to that of the undertaking which controls the existing product or service.

It follows that, for the purposes of examining whether the refusal by an undertaking in a dominant position to grant a licence for a brick structure protected by an intellectual property right which it owns is abusive, the degree of participation by users in the development of that structure and the outlay, particularly in terms of cost, on the part of potential users in order to purchase studies on regional sales of pharmaceutical products presented on the basis of an alternative structure are factors which must be taken into consideration in order to determine whether the protected structure is indispensable to the marketing of studies of that kind.

(see paras 28, 30, operative part 1)

3. The refusal by an undertaking which holds a dominant position and owns an intellectual property right in a brick structure indispensable to the presentation of regional sales data on pharmaceutical products in a Member State to grant a licence to use that structure to another undertaking, which also wishes to provide such data in the same Member State, constitutes an abuse of a dominant position within the meaning of Article 82 EC where the following conditions are fulfilled:

- the undertaking which requested the licence intends to offer, on the market for the supply of the data in question, new products or services not offered by the owner of the intellectual property right and for which there is a potential consumer demand;

- the refusal is not justified by objective considerations;

- the refusal is such as to reserve to the owner of the intellectual property right the market for the supply of data on sales of pharmaceutical products in the Member State concerned by eliminating all competition on that market.

(see para. 52, operative part 2).

**Case T-201/04 Microsoft Corp. v Commission of the European Communities**

1. Where the national courts give a ruling on agreements or practices which may subsequently be the subject of a decision by the Commission, they must avoid taking decisions which conflict with those taken or envisaged by the Commission in the implementation of Articles 81 and 82 EC.

(see para. 19)

2. In the assessment of the abusive character of a dominant position, in order to determine whether a product or service is indispensable for enabling an undertaking to carry on business in a particular market, it must be determined whether there are products or services which constitute alternative solutions, even if they are less advantageous, and whether there are technical, legal or economic obstacles capable of making it impossible or at least unreasonably difficult for any undertaking seeking to operate in the market to create, possibly in cooperation with other operators, alternative products or services. In order to accept the existence of economic obstacles, it must be established, at the very least, that the creation of those products or services is not economically viable for production on a scale comparable to that of the undertaking which controls the existing product or service.

It follows that, for the purposes of examining whether the refusal by an undertaking in a dominant position to grant a licence for a brick structure protected by an intellectual property right which it owns is abusive, the degree of participation by users in the development of that structure and the outlay, particularly in terms of cost, on the part of potential users in order to purchase studies on regional sales of pharmaceutical products presented on the basis of an alternative structure are factors which must be taken into consideration in order to determine whether the protected structure is indispensable to the marketing of studies of that kind.

(see paras 28, 30, operative part 1)
meaning of Article 82 EC where the following conditions are
fulfilled:

- the undertaking which requested the licence intends to offer,
on the market for the supply of the data in question, new
products or services not offered by the owner of the
intellectual property right and for which there is a potential
consumer demand;

- the refusal is not justified by objective considerations;

- the refusal is such as to reserve to the owner of the
intellectual property right the market for the supply of data on
sales of pharmaceutical products in the Member State
concerned by eliminating all competition on that market.
(see para. 52, operative part 2).
III. Law of domain names

Uniform Domain Name Dispute Resolution Policy

[As Approved by ICANN on October 24, 1999]

1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us ([the registrar]) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at www.icann.org/udrp/udrp-rules-24oct99.htm, and the selected administrative-dispute-resolution service provider’s supplemental rules.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.

3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:
   a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;
   b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
   c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.


This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that
   (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
   (ii) you have no rights or legitimate interests in respect of the domain name; and
   (iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:
   (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or
   (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or
   (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
   (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

   (i) your domain name is identical or confusingly similar to a trademark or service mark in which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)
   (ii) you have no rights or legitimate interests in respect of the domain name; and
   (iii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or
   (iv) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
   (v) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of your web site or location.

   We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.
(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel’s decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 5 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.
9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration.

---

**Rules for Uniform Domain Name Dispute Resolution Policy**

As approved by the ICANN Board of Directors on 30 October 2009.

These Rules are in effect for all UDRP proceedings in which a complaint is submitted to a provider on or after 1 March 2010. The prior version of the Rules, applicable to all proceedings in which a complaint was submitted to a Provider on or before 28 February 2010, is at [http://www.icann.org/en/dndr/udrp/unifbrn-rules-24oct99-en.htm](http://www.icann.org/en/dndr/udrp/unifbrn-rules-24oct99-en.htm). UDRP Providers may elect to adopt the notice procedures set forth in these Rules prior to 1 March 2010.

Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.

Definitions

In these Rules:

Complainant means the party initiating a complaint concerning a domain-name registration.

ICANN refers to the Internet Corporation for Assigned Names and Numbers.

Mutual Jurisdiction means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder’s address as shown for the registration of the domain name in Registrar’s Whois database at the time the complaint is submitted to the Provider.

Panel means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

Panelist means an individual appointed by a Provider to be a member of a Panel.

Party means a Complainant or a Respondent.

Policy means the Uniform Domain Name Dispute Resolution Policy that is incorporated by reference and made a part of the Registration Agreement.

Provider means a dispute-resolution service provider approved by ICANN. A list of such Providers appears at [http://www.icann.org/en/dndr/udrp/approved-providers.htm](http://www.icann.org/en/dndr/udrp/approved-providers.htm).

Registrar means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

Registration Agreement means the agreement between a Registrar and a domain-name holder.

Respondent means the holder of a domain-name registration against which a complaint is initiated.

Reverse Domain Name Hijacking means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

Supplemental Rules means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, file size and format modalities, the means for communicating with the Provider and the Panel, and the form of cover sheets.

Written Notice means hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or of any annexes.

Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider’s responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name’s registration data in Registrar’s Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration’s billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) postmaster@<the contested domain name>.; and
(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant under Paragraph 3(b)(v).

(b) Except as provided in Paragraph 2(a), any written communication to Complainant or Respondent provided for under these Rules shall be made electronically via the Internet (a record of its transmission being available), or by any reasonably requested preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) and 5(b)(iii)).

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including, where applicable, the number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11.

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable or, where applicable

(ii) if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or:

(iii) if by postal or courier service, on the date marked on the receipt.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with Paragraph 2(f).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(j) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes. This includes the Provider in sending Written Notice to the Respondent by post and/or facsimile under Paragraph 2(a)(i).

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).

The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN. (Due to capacity constraints or for other reasons, a Provider's ability to accept complaints may be suspended at times. In that event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint including any annexes shall be submitted in electronic form and shall:

(i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a);

(vi) Specify the domain name(s) that is/are the subject of the complaint;

(vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;

(viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with which it intends, at the time the complaint is submitted, to use the mark in the future); and

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having been registered and being used in bad faith...
(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) and 4(c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that a copy of the complaint, including any annexes, together with the cover sheet prescribed by the Provider's Supplemental Rules, has been sent or transmitted to the Respondent (domain-name holder), in accordance with Paragraph 2(b);

(xiii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiv) Conclude with the following statement followed by the signature (in any electronic format) of the Complainant or its authorized representative:

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

(xv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

Notification of Complaint
(a) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint, including any annexes, electronically to the Respondent and shall send Written Notice of the complaint (together with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by Paragraph 2(a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with Paragraph 19.

(b) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(c) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) in connection with sending the complaint to the Respondent.

(d) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN of the date of commencement of the administrative proceeding.

The Response
(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider;

(b) The response, including any annexes, shall be submitted in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) If Complainant has elected a single-member panel in the complaint (see Paragraph 3(b)(iv)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(vii) State that a copy of the response including any annexes has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b); and

(viii) Conclude with the following statement followed by the signature (in any electronic format) of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.
(c) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider’s Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(d) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.

(e) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel (Paragraphs 3(b)(iv) and 5(b)(iv)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in Paragraph 6(e). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN-approved Provider’s list of panelists.

(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party’s list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider’s selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider’s submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case administrator appointed by the Provider in the manner prescribed in the Provider’s Supplemental Rules.

Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

Language of Proceedings

(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under,
these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

Panel Decisions
(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to Paragraph 6.

(c) In the case of a three-member Panel, the Panel’s decision shall be made by a majority.

(d) The Panel’s decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider’s Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of Paragraph 4(a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

Communication of Decision to Parties
(a) Within three (3) calendar days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN. The concerned Registrar(s) shall immediately communicate to each Party, the Provider, and ICANN the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see Paragraph 4(f) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see Paragraph 15(e) of these Rules) shall be published.

Settlement or Other Grounds for Termination
(a) If, before the Panel's decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding.

(b) If, before the Panel's decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

Effect of Court Proceedings
(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

(b) In the event that a Party initiates any legal proceedings during the pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See Paragraph 8 above.

Fees
(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider's Supplemental Rules, within the time and in the amount required. A Respondent electing under Paragraph 5(b)(iv) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See Paragraph 5(c). In all other cases, the Complainant shall bear all of the Provider’s fees, except as prescribed under Paragraph 19(d). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider’s Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with Paragraph 19(a).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.

(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

Exclusion of Liability
Except in the case of deliberate wrongdoing, neither the Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

Amendments
The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN.

Uniform Domain Name Resolution Policy – Relevant Case Law

America Online, Inc. v. Johuathan Investments, Inc., and AOLNEWS.COM Case No. D 2001-0918

1. The Parties

The Complainant is America Online, Inc., 22000 AOL Way, Dulles, Virginia 20166, USA and represented by James R. Davis II, Arent Fox Kintner Plotkin & Kahn, 1050 Connecticut Avenue, NW, Washington, DC 20036, USA.

The Respondent is Johuathan Investments, Inc., and AOLNEWS.COM, 62 Cleighorn Street, Belize City, Belize.
2. The Domains Name and Registrars

The Domain Names are <aolnews.com> and <fucknetscape.com>.

The Registrars are TuCows.com, Inc., and BulkRegister.com, Inc.

3. Procedural History

The Complaint was received by WIPO by email on July 17, 2001, and in hardcopy form on July 19, 2001. WIPO issued a Request for Amendment to Complaint on July 27, 2001. The Amended Complaint was received by email on July 30, 2001, and in hard copy form on August 3, 2001. WIPO has verified that the Complaint satisfies the formal requirements of the Policy, the Rules and the Supplemental Rules and that payment was properly made. The Administrative Panel ("the Panel") is satisfied that this is the case.

The Complaint was properly notified in accordance with the Rules, paragraph 2(a). BulkRegister.com, Inc., has confirmed that <aolnews.com> ("the First Domain Name") was registered through BulkRegister.com, Inc. and that AOLLNEWS.COM is the current registrant, TuCows.com, Inc., has confirmed that <fucknetscape.com> ("the Second Domain Name") was registered through TuCows.com, Inc., and that Johuathan Investments, Inc. is the current registrant. The Registrars have further confirmed that the Policy is applicable to the Domain Names.

For the reasons set out below the Panel treats aollnews.com as being a trading name or ‘alter ego’ of Johuathan Investments, Inc. and hereinafter refers to them both as “the Respondent”.

On August 6, 2001, WIPO notified the Respondent of the Complaint in the usual manner and informed the Respondent inter alia that the last day for sending its Response to the Complainant and to WIPO was August 26, 2001. No Response was received.

The Panel was properly constituted. The undersigned Panelist submitted Statements of Acceptance and Declarations of Impartiality and Independence.

No further submissions were received by WIPO or the Panel, as a consequence of which the date scheduled for the issuance of the Panel’s Decision is September 17, 2001.

4. Factual Background

The Complainant is America Online, Inc., and hereinafter refers to them both as "AOL".

AOL is the proprietor of many trade mark registrations of or incorporating the marks AOL and Netscape.

AOL has been using the mark AOL since at least as early as 1989 and the mark NETSCAPE since at least as early as 1984. Both marks are very well known marks in the area of computer online services and other internet related services. Moreover, they were very well known at the time the Domain names were registered.

Further, AOL is the registered proprietor of trade mark registrations for the mark AOL.COM, a mark it has used since at least 1992, and operates a website at (inter alia) www.aolnews.com.

The First Domain Name was registered on June 13, 2000, in the name of aollnews.com. The Second Domain Name was registered on April 23, 2000, in the name of Johuathan Investment Inc. The registrants have different names, but they have the same address in Belize and both have the same contact addresses and telephone numbers.

The Domain Names are connected (directly or indirectly) to commercial sites. The First Domain Name is connected to a website at <point.com>. The Second Domain Name is connected to a pornographic website. Neither of these sites contains any reference within it to either aollnews or fucknetscape.

5. Parties’ Contentions

A. Complainant

The Complainant contends that aollnews.com, the registrant of the First Domain Name, and Johuathan Investments, Inc., the registrant of the Second Domain Name, are one and the same and that it is appropriate this complaint should be entertained as a single complaint on the basis that there is a single respondent to the complaint. The Complainant points to the similarities in the various addresses and telephone numbers in the Whois records for the Domain Names.

The Complainant contends that the Domain Names are each nearly identical and are each confusingly similar to a trade mark or service mark in which the Complainant has rights. The Complainant refers to its rights in the trade marks AOL, AOL.COM and NETSCAPE. It also refers to the AOL operated website at <aolnews.com>.

The Complainant contends that at the time of registering the Domain Names the Respondent was well aware of the Complainant’s rights in the aforementioned trade marks.

The Complainant contends that consumers will be likely to believe that, because of the Respondent’s use of the Complainant’s famous trade marks, the Complainant is in some way associated with the website. The Complainant points to the additional fact that the Whois search for the Second Domain Name shows that the Respondent uses an aol.com email address which will be likely to increase the risk of confusion. The Complainant also points to the fact that the site connected to the First Domain Name offers services similar to those offered by AOL.

The Complainant contends that the Respondent registered the Domain Names with a view to capitalising on the fame of the Complainant’s trade marks.

The Complainant asserts that the Respondent has no rights or legitimate interest in respect of the Domain Names. It says that it has not granted a licence to the Respondent to use any of its marks. Further it claims that in light of what is set out in this Complaint the Respondent cannot claim in good faith that it has made a non-commercial or fair use of the Domain Names or that it is commonly known by the name AOL, Aollnews, or Netscape.

The Complainant contends that the Domain Names were registered in bad faith and are being used in bad faith.

In support, the Complainant refers to the matters set out above. The Complainant adds that the Domain Names are being used to attract commercial attention and not to define the content of the sites at <aolnews.com> and <fucknetscape.com>.

The Complainant further refers to the fact that in a previous ICANN proceeding (FA0012000096178 Sunglass Huet Corporation v. Johuathan Investments Inc) the Registrant was found guilty of registering the Domain Name in bad faith and using it in bad faith. The Complainant cites the case in support of a contention that it demonstrates a pattern on the part of
the Respondent to register domain names with a view to preventing trade mark owners from reflecting those marks in corresponding domain names. The Complainant asserts that this is in violation of paragraph 4(b)(i) of the Policy.

The Complainant further contends that the use of famous marks of others, particularly when connected to adult material, violates the Policy.

B. Respondent

The Respondent has not responded.

6. Discussion and Findings

According to paragraph 4(a) of the Policy, the Complainant must prove that

(i) the Domain Name is identical or confusingly similar to a trade mark or service mark in which the Complainant has rights; and

(ii) the Respondent has no rights or legitimate interest in respect of the Domain Name; and

(iii) the Domain Name has been registered and is being used in bad faith.

First, however, the Panel has to decide whether or not it was appropriate for this complaint to be entertained in circumstances where the named registrants for the Domain Names have different names. The Complainant’s assertion that the registrants are in effect one and the same is clear. The Panel believes it more than likely that the registrants are one and the same, but recognises that it is not impossible that the address is an accommodation address for a multiplicity of different entities.

The Respondent has elected not to respond. By virtue of Rule 14(b) the Panel is entitled to draw such inferences as it deems appropriate from the failure to respond. In the circumstances the Panel sees no reason not to accept the Complainant’s uncontradicted assertion that the registrants of the Domain Names are one and the same. The Panel accepts this complaint as a properly constituted single complaint covering both Domain Names.

Identical or Confusing Similarity

The First Domain Name <aollnews.com>. This Domain Name comprises “AOLL”, which is very similar to the Complainant’s trade mark AOL, the term “NEWS”, which is generic, and the generic dot com suffix. In combination the First Domain Name is very similar indeed to the Complainant’s domain name, <aolnews.com>, under and by reference to which the Complainant provides a service. The Panel finds that this Domain Name is confusingly similar to trade marks and service marks in which the Complainant has rights.

The Second Domain Name <fucknetscape.com>. This Domain Name comprises the word “FUCK”, the Complainant’s trade mark “NETSCAPE” and the generic dot com suffix. This Domain Name is not identical to the Complainant’s trade mark, but is it confusingly similar to it?

In the trade mark context the term “confusingly similar” refers to confusion as to trade origin. Is it likely therefore that, because of the similarity between the Domain Name on the one hand and the Complainant’s trade mark on the other hand, people will believe that the Domain name is associated in some way with the Complainant?

The Panel regards it as inconceivable that anyone looking at this Domain Name will believe that it has anything to do with a company of such high repute as the Complainant. It is manifestly, on its face, a name, which can have nothing whatever to do with the Complainant. It is a name, which, by its very nature, declares that it is hostile to Netscape. The Panel notes that in support of the bad faith claim the Complainant contends that the Respondent has registered this Domain Name in violation of paragraph 4(b)(ii) of the Policy on the basis that it has been done to prevent the Complainant registering the name. The Panel simply does not understand why on earth the Complainant would ever wish to register this Domain Name. There is no evidence before the Panel to support the contention. The Panel is aware that some companies seek to acquire such names, but only to forestall and/or impede the more obvious protest sites, not because they believe people will believe that the domain name in question or any site to which it is connected belongs to or is licensed or endorsed by the trade mark owner.

The Panel finds that the Complainant has failed to prove that this Domain Name is identical or confusingly similar to a trade mark or service mark in which the Complainant has rights.

Rights or Legitimate Interest of the Respondent

The Complainant asserts that it has not granted any licence to the Respondent to use the Complainant’s trade marks. The Panel accepts that uncontradicted assertion. The Panel observes that there can be no reason why the Complainant would license use of its trade marks in relation to either of the domain names, one of which includes a mis-spelling and the other of which is offensive.

The Policy gives a respondent an opportunity to demonstrate to the Panel that it has rights or legitimate interests in respect of the domain names in issue. A non-exhaustive list of circumstances, which demonstrate the existence of such rights and legitimate interests, is set out in paragraph 4(c) of the Policy.

The Respondent has made no attempt to demonstrate any of those circumstances or indeed any other circumstances showing that it has rights or legitimate interests in respect of the Domain Names.

The Panel can think of no reason why the Respondent could be said to have rights or legitimate interests in respect of the Domain Names, save that aollnews.com is the registered name of the owner of the First Domain Name.

However, the circumstances are such that the Respondent clearly selected the Domain Names with the Complainant in mind, evidently well aware of the Complainant’s trade mark interests in relation to them. The Panel is of the view that the business name, aollnews.com, was selected as a convenient alias for the purpose in hand and is no evidence that the Respondent has been commonly known by that name within the meaning of paragraph 4(c)(ii) of the Policy.

The Panel finds that the Respondent has no rights or legitimate interests in respect of either of the Domain Names.

Bad Faith

The First Domain Name <aollnews.com>. The circumstances are such that the Respondent knew when it registered this Domain name that it was confusingly similar to the Complainant’s trade marks and domain name <aolnews.com> referred to above. The Respondent also knew that it had no rights or legitimate interests in respect of this Domain Name. This Domain Name is connected to a commercial site. In the absence of any explanation from the Respondent, the Panel is entitled to infer that the Respondent intended, for a
commerical purpose, the natural and probable consequences of having effected the registration, namely confusion of internet users. In the result, the Panel finds that the First Domain Name was registered in bad faith and is being used in bad faith within the meaning of paragraph 4(b)(iv) of the Policy.

The Second Domain Name <fucknetscape.com>. Given the Panel's finding in relation to paragraph 4(a)(i) of the Policy, it is not necessary for the Panel to address this issue. For the record, however, and for the reasons set out above, the Panel rejects the Complainant's contentions that this Domain Name will be likely to lead to any relevant confusion of internet users or has in any way precluded the Complainant from registering a domain name of its choice. If there is any confusion, it will be because people expecting to visit a protest site will find themselves at a porn site. In an obvious sense, perhaps, the registration of this Domain Name is an abuse of the Domain Name System, but not an abuse of a kind covered by the Policy.

For completeness, the Panel addresses the contention by the Complainant that the content of the site to which the domain name in question is connected may have a bearing on the bad faith issue "particularly in connection with adult content". The Panel accepts that the content of a site (adult or otherwise) might well be of relevance to indicate a respondent's good faith/bad faith intentions, but each of the authorities cited by the Complainant in relation to adult material proceeds upon the basis that the domain name in issue is confusingly similar to the Complainant's trade mark. In the case of the Second Domain Name the Panel has found that the Complainant has failed to prove confusing similarity.

7. Decision

In light of the foregoing findings the complaint in respect of the First Domain Name succeeds and the Panel directs that the Domain Name, <aollnews.com>, be transferred to the Complainant. The complaint in respect of the Second Domain Name, <fucknetscape.com>, is dismissed.

Tony Willoughby
Sole Panelist

Dated: September 14, 2001

Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale Case No. D2000-0662

1. The Parties

The Complainant is Wal-Mart Stores, Inc., a United States corporation with its headquarters in Bentonville, Arkansas, United States of America.

The Respondent is Richard MacLeod d/b/a For Sale, 21 Simpson Avenue, Toronto, ON M8Z1C9, United States of America.

2. The Domain Name and Registrar

The domain name at issue is walmartuksucks.com. The domain name is registered with Register.com.

3. Factual Background

The Panel has reviewed the Complainant's Complaint and Respondent's Response. The following facts appear to be undisputed: The Complainant operates over 2,500 stores worldwide. All its trading operations, advertisements and promotions are conducted under the mark "Wal-Mart," and it has used this mark continuously since 1962. Its Internet addresses include walmart.com, wal-mart.com, and walmartstores.com. Its businesses include discount retail stores, grocery stores, pharmacies, membership warehouse clubs, and deep discount warehouse outlets.

Complainant holds registrations for the mark "Wal-Mart" in the United States, Switzerland, the United Kingdom, Denmark, and numerous other countries. The Respondent has no rights granted by the Complainant in any of the marks involving the word "Wal-Mart".

The Respondent registered the domain name walmartuksucks.com on February 12, 2000. Complainant filed its Complaint by email on June 22, 2000. Because of a deficiency noted by the Center (Complainant had failed to comply with Rule 3(b)(ix)), Complainant filed an Amended Complaint, which was received in hardcopy by the Center on July 10, 2000. On July 14, 2000, the Center formally commenced this proceeding and notified Respondent that its Response would be due by August 2, 2000. Respondent timely filed its Response, which was received by the Center in hardcopy on July 26, 2000. Meanwhile, on July 20, 2000, the Center released a decision in Wal-Mart Stores, Inc. v. Walsucks and Walmart Puerto Rico, Case No. D2000-0477, which involved the same Complainant. The Panel in that case ruled that the domain names wal-martsucks.com, walmartcanadasucks.com, walmartuk2sucks.com, walmartpuertoricosucks.com were confusingly similar to Complainant’s Wal-Mart trademark, that the respondent in that case lacked a legitimate interest in the domain names, and that the domain names were registered and used in bad faith. The Panel thus ordered that the domain names be transferred to the Complainant.

On July 25, 2000, Complainant in this case requested leave to submit a reply in light of the decision in Case No. D2000-0447. On July 26, 2000, the Respondent indicated that he would not object to the filing of a reply, and requested that he be allowed to submit a sur-reply.

On August 4, 2000, the Center appointed a Panel. The Panelist thereafter developed a conflict of interest, and recused himself. On September 6, 2000, the Center appointed David H. Bernstein as a substitute Panelist. Neither party requested a three-member Panel.

On September 6, 2000, the Panel issued an order denying the Complainant's request for leave to file a reply, except that the Panel took note of the decision in Case No. D2000-0447, and denying as moot the Respondent's request to submit a sur-reply. On September 17, 2000, the Respondent asked that he be allowed to submit a statement regarding Case No. D2000-0447. In particular, Respondent requested the right to supplement his Response because, "[s]hould this case be used against me, I believe it would be fair to give me a chance to submit a few comments about that case." The Panel denies Respondent's request to supplement his Response. First, the request is moot because Case No. D2000-0447 has not been "used against" him; the issues in this case are quite different and, although this Panel has read the decision in Case No. D2000-0447, that decision has not affected the Panel's findings and conclusions in this case. More generally, Respondent's request is inconsistent with the expedited process created by ICANN. If parties were allowed to supplement their submissions based solely on the issuance of a decision by another Panel, it would, given the pace with which UDRP decisions are issued, allow parties endlessly to drag out the UDRP process with replies and sur-replies and sur-sur-replies. See Document Technologies, Inc. v.
International Electronic Communications, Inc., Case No. D2000-0270 (WIPO, June 6, 2000) (denying Complainant’s request to file reply where proposed reply raised no new legal or factual authority, and thus would unnecessarily delay the final adjudication). When a new, relevant decision is issued (whether by another Panel or by a court), the appropriate course instead is for a party to bring the decision to the Panel’s attention, without providing additional, substantive argument, so that the Panel can review the decision and use its own judgment as to whether that decision is relevant to the issues in the case before the Panel and, if so, how it affects the decision in the instant case. See Pet Warehouse v. Pets.Com, Inc., Case No. D2000-0105 (WIPO, Apr. 13, 2000) (accepting supplemental submission comprised of a new decision by another UDRP Panel that was submitted "without any argument").

Discussion and Findings

5. Parties’ Allegations

The Complainant submits that its mark is famous throughout the United States and all those other countries in which it trades. It further argues that the domain name is identical to its “Wal-Mart” mark because the domain name wholly incorporates "Wal-Mart" and also is confusingly similar to its "Wal-Mart" marks because "Wal-Mart" is so famous that buyers "would be likely to think that any commercial site connected with the domain name wal-martsucks.com, particularly a site selling consumer products," or “any domain name incorporating the Wal-Mart name (or a close approximation thereof)” originates with the Complainant.

The Complainant argues that Respondent has no rights or legitimate interests in respect of the domain name. First, Respondent is not currently using the domain name in connection with any ongoing business. Second, to the best of the Complainant’s knowledge, Respondent has no rights to any use of the term Wal-Mart.

The Complainant further submits that the domain name wal-martsucks.com was registered and is used in bad faith. Improper use of the name is shown by the Respondent’s attempt to sell the name through the Great Domains website for $530,000 and on Respondent’s website for $545,000.

The Respondent argues that the Panel should find that the Policy is to prove:

(a) That the domain name registered by the Respondent is identical or confusingly similar to a trademark or service mark in which the Complainant has rights;
(b) That the Respondent has no rights or legitimate interests in respect of the domain name; and
(c) The domain name has been registered and used in bad faith.

Initially, the Panel rejects any suggestion that Complainant’s failure to register wal-martsucks.com before Respondent did so precludes this Complaint under any theory, including laches. Trademark owners are not required to create "libraries" of domain names in order to protect themselves, and there are strong policy reasons against encouraging this behavior. Moreover, as human creativity reaches its utmost where disparagement (not to mention money) is involved, any such attempt by a trademark owner would be futile, and thus Respondent has no equitable argument against Complainant.

The second and third elements of the Policy are easily disposed of in this case. Respondent’s sole argument with respect to the second element is that he is using wal-martsucks.com to criticize Wal-Mart. Respondent could potentially have a legitimate interest in using wal-martsucks.com as a site critical of Wal-Mart; the Policy specifically provides that "a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark," can establish legitimate rights and interests in a domain name. Policy paragraph 4(c)(iii). In this case, however, Complainant alleges, and Respondent does not deny, that before Complainant initiated the present proceeding, he was using the site solely for the purpose of selling it. While Respondent claims to have had a "change of heart," this change appears to have been driven by his domain name dispute with Complainant, and it is too little, too late.

Respondent admits that he registered the domain name in bad faith. The Panel specifically rejects Respondent’s argument that Complainant produced insufficient evidence of bad faith use. Though Respondent questions the reliability of the information on the Great Domains website (Respondent claims that anyone can list a domain name for sale on that site, and thus Complainant has not proven that it is Respondent who offered the name for sale), he never actually denies that it was he who listed wal-martsucks.com on Great Domains, nor does he deny that he offered the domain name for sale on his own site. Indeed, the Respondent’s intent is made clear by the name in which he registered the domain name: "For Sale." See Unibanco v. Vendo Domain Sale, Case No. D2000-0671 (WIPO, Aug. 31, 2000). Combined with Respondent’s own admission, this is ample evidence of bad faith use. Again, Respondent’s newly developed critical use of the site during the pendency of this proceeding is insufficient to erase the prior bad faith use.

The difficult question in this case is whether Complainant has shown that wal-martsucks.com “is identical or confusingly similar to” Complainant’s mark under Paragraph 4(a)(1) of the Policy. In prior cases, this Panel has held that a domain name that incorporates a mark but also adds another word is not “identical” to the mark under the Policy. See, e.g., EA Auto, L.L.C. v. Triple S. Auto Parts d/b/a King Fu Yea Enterprises, Inc., No. D2000-0047 (WIPO, Mar. 24, 2000). This Panel has also held that incorporating a distinctive mark in its entirety creates sufficient similarity between the mark and the domain name to render it confusingly similar. Id.

Following this reasoning, Complainant contends that consumers are likely to believe that any domain name incorporating the sequence “Wal-Mart” or a close approximation thereof is associated with Complainant. In the ordinary case, when a generic term is appended to the
trademark (such as the domain name walmartstores.com), this would be so. But the fame of a mark does not always mean that consumers will associate all use of the mark with the mark's owner. No reasonable speaker of modern English would find it likely that Wal-Mart would identify itself using wal-martsucks.com. Complainant has no evidence of any potential confusion. The Panel specifically rejects Complainant's argument that consumers are likely to be confused as to the sponsorship or association of a domain name that combines a famous mark with a term casting opprobrium on the mark.

Nevertheless, the Panel understands the phrase "identical or confusingly similar" to be greater than the sum of its parts. The Policy was adopted to prevent the extortionate behavior commonly known as "cybersquatting," in which parties registered domain names in which major trademark owners had a particular interest in order to extort money from those trademark owners. This describes Respondent's behavior. Thus, the Panel concludes that a domain name is "identical or confusingly similar" to a trademark for purposes of the Policy when the domain name includes the trademark, or a confusingly similar approximation, regardless of the other terms in the domain name. In other words, the issue under the first factor is not whether the domain name causes confusion as to source (a factor more appropriately considered in connection with the legitimacy of interest and bad faith factors), but instead whether the mark and domain name, when directly compared, have confusing similarity. Having so concluded, Respondent's use of the domain name wal-martsucks.com meets all three of the conditions necessary to justify a transfer of the domain name to Complainant.

The Panel is cognizant of the importance of protecting protest sites that use a trademark to identify the object of their criticism. The "legitimate interest" and "bad faith" factors should adequately insulate true protest sites from vulnerability under the Policy, especially as the Complainant retains the burden of proof on each factor. Where, as here, a domain name registrant does not use a site for protest but instead offers it for sale for substantially more than the costs of registration, the site does not further the goal of legitimate protest; rather, it constitutes trademark piracy.

7. Decision

For the foregoing reasons, the Panel decides:

(a) that the domain name wal-martsucks.com is identical or confusingly similar to the Wal-Mart trademark in which the Complainant has rights;

(b) that the Respondent has no rights or legitimate interests in respect of the domain name; and

(c) the Respondent's domain name has been registered and is being used in bad faith.

Accordingly, pursuant to paragraph 4(i) of the Policy, the Panel requires that the registration of the domain name wal-martsucks.com be transferred to the Complainant.

David H. Bernstein
Sole Panelist

Dated: September 19, 2000

FC Bayern München AG v. Peoples Net Services Ltd. Case No. D2003-0464

1. The Parties

The Complainant is FC Bayern München AG, of Munich, Germany, represented by Beiten Burkhardt Goerdeler of Germany.

The Respondent is Peoples Net Services Ltd., Mr. Sam Rosen, Director, of London, United Kingdom of Great Britain and Northern Ireland.

2. The Domain Names and Registrar

The disputed domain names <bayernmunchen.net> and <bayernmunchen.net> are registered with Domain Bank.

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on June 26, 2003. On June 18, 2003, the Center transmitted by email to Domain Bank a request for registrar verification in connection with the domain names at issue. On June 19, 2003, Domain Bank transmitted by email to the Center its verification response confirming that the Respondent is listed as the registrant and providing the contact details for the administrative and technical contact. The Center verified that the Complaint satisfied the formal requirements of the Uniform Domain Name Dispute Resolution Policy (the "Policy"), the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"), and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the "Supplemental Rules").

In accordance with the Rules, paragraphs 2(a) and 4(a), the Center formally notified the Respondent of the Complaint, and the proceedings commenced on June 24, 2003. In accordance with the Rules, paragraph 5(a), the due date for Response was July 14, 2003. The Response was filed with the Center on June 24, 2003.

The Center appointed Peter G. Nitter as the sole panelist in this matter on July 1, 2003. The Panel finds that it was properly constituted. The Panel has submitted the Statement of Acceptance and Declaration of Impartiality and Independence, as required by the Center to ensure compliance with the Rules, paragraph 7.

4. Factual Background

The Complainant is FC Bayern München AG, a stock corporation which since 2002, operates the soccer activities of FC Bayern München e.V., a registered association founded in 1900.

All trademarks and name rights formerly held by FC Bayern München e.V. were transferred to FC Bayern München AG on January 5, 2002.

The Complainant has activities in all major sports, but is particularly known for its football team. The football team Bayern Muenchen is one of the most successful teams in the world and the most famous team in Germany.

The Complainant's trademark FC BAYERN MÜNCHEN EV with the club logo forms the subject-matter of trademark registrations in about 30 countries. Among these is a registration in the UK (register no. 2004623) with a priority date of November 4, 1994, inter alia registered for numerous merchandising goods and printed matter, and a Community Trademark CTM000494187 with a priority date of November 23, 1998.

The Complainant uses the trademarks by granting the right to use the trademark to a third party (licensing). The licensees

Institute of Law and Technology
Masaryk University, Faculty of Law
produce and distribute a wide variety of products with the trademarks.

5. Parties’ Contentions
A. Complainant
Confusingly Similar
BAYERN MÜNCHEN is the specifying part of the club logo. Apart from the specifying part, the logo contains two descriptive elements: "FC" is the abbreviation for "football club" and "e.V." stands for "registered association".

BAYERN MÜNCHEN is also the name of the Complainant.

The Complainant has a worldwide reputation and is also very well-known in the UK.

A study done by a consulting firm presented by the Complainant concluded that the Complainant is in the Top Ten of the world’s best-known and most valuable brand names in sports.

As the letter (umlaut) "ü" is not used outside Germany, the common international way to spell words with umlauts is to replace the "ü" by "ue", so that it reads "Bayern Muenchen". This in particular applies to domain names, as umlauts cannot be used in domain names. Sometimes, the dots on the "ü" are overlooked, and the "ü" is simply replaced by a "u", so that it reads "Bayern Munchen". Both ways to spell the name are common and widely used.

The Complainant is also the registered owner of numerous international Internet domains which contain its name, for example these which are most similar to the domain name in dispute:

<bayernmuenchen.com>
<bayernmuenchen.de>
<bayern-muenchen.com>

The domain names <bayernmuenchen.net> and <bayernmunchen.net> are nothing but the international spelling of "Bayern München" and thus identical to the specifying part of the numerous trademarks of the Complainant used worldwide.

No Rights or Legitimate Interests
The Respondent has no legitimate right to use the disputed domain names.

The Respondent is not commonly known by the domain names.

The Respondent offers email services, where the user can choose from "hundreds of domain names". The Respondent offers approximately 1600 domain names, including several which includes the word "football" etc.

With the commercial service provided by the Respondent, any user who is willing to pay the fees may use an email address with any of the domain names as the last part of an email address. Accordingly, the Respondent also offers email addresses like john@bayernmuenchen.net and tickets@bayernmuenchen.net.

The use of such email addresses may lead to considerable confusion as it appears to be an official email address of the Complainant itself. The use of such email addresses is beyond the control of the Complainant and endangers the reputation of the name and trademarks of the Complainant.

The Respondent also makes use of the well-known name for his own business activities. Any user who enters the sites at the disputed domain names is led to the web page of the Respondent, on which he offers his commercial service. This is an obvious attempt to divert customers and fans of the Complainant to promote the business of the Respondent.

Bad Faith
The domain names clearly refer to the Complainant as the famous soccer club.

When registering the domain names, it was of course known to the Respondent that these domains use the name of the world-famous soccer club. The Complainant is also famous in the UK.

The Respondent is familiar with football, as his other football domains demonstrate.

The Respondent intentionally attempted to attract, for commercial gain, Internet users to the Respondent's web site by creating a likelihood of confusion with the Complainant's mark and name as to the sponsorship, affiliation, or endorsement of the Respondent's web site or the services constituting the Respondent's business activities. The Respondent hoped that soccer fans would want to use an email address with the name of their favorite club, and thus attempted to use the famous name of the Complainant for his own profit.

B. Respondent
Confusingly Similar
The Complainant may have registered trademarks identical to the disputed domain names for Football Club purposes and associated activities only.

The disputed domains mean Bavaria Munich and are therefore generic in nature like Paris France or London England.

The Respondent never sought to use the domains in any connection with the Complainant's business or other activities.

Rights or Legitimate Interests
The Respondent has full rights over the disputed domain names as they are generic in nature and in the public domain in so far as they relate to geographical place names.

Bad Faith
The disputed domain names have never nor will ever be used in bad faith. They are currently used to provide e-mail addresses to our customers of "www.Okmail.com". There has never been an offer by the Respondent to sell or otherwise transfer the domains to the Complainant.

6. Discussion and Findings
Paragraph 4(a) of the Policy lists three tests, which a complainant must satisfy in order to succeed. The Complainant must satisfy that:

(i) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) the respondent has no rights or legitimate interests in respect of such domain name; and

(iii) the domain name has been registered and is being used in bad faith.

A. Identical or Confusingly Similar
The domain names in dispute are <bayernmuenchen.net> and <bayernmunchen.net>. 
The Complainant’s trademark is FC BAYERN MÜNCHEN E.V. with the club logo is registered in about 30 countries. Among these, there is a registration in the UK (register no. 2048623) with a priority date of November 4, 1994, and a Community Trademark CMI000494187 with a priority date of November 23, 1998.

The two descriptive elements in the trademark: "FC" which is the abbreviation for "football club" and "e.V." which stands for "registered association" can not be taken into account.

The conclusion is that the disputed domain names both are confusingly similar to Complainant’s registered trademarks.

B. Rights or Legitimate Interests

The disputed domain names contain geographical place names. But in the Panel’s opinion the name BAYERN MÜNCHEN has a secondary meaning, namely the famous soccer club of the Complainant.

The Respondent is not commonly known by the domain names.

The Respondent uses the well-known name BAYERN MÜNCHEN for his own business activities, which has no connection to the geographical areas Bayern or München. The Respondent offers commercial email services on the sites which the domain names leads to. The Panel finds that this is an attempt to divert Internet users for commercial gain.

A user who enters the Respondent’s sites can choose from a large number of domain names. A user who pays the fees can use an email address with any of the domain names as the last part of an email-address. The Respondent offers email addresses like tickets@bayernmuenchen.net, which may lead to considerable confusion as it appears to be an official email address of the Complainant itself.

The Respondent has no right or legitimate interests to use the disputed domain names.

C. Registered and Used in Bad Faith

There is no evidence that the Respondent has offered to sell or otherwise transfer the domains to the Complainant.

However, the domain name include the well-known name of the Complainant and the well-known trademarks of the Complainant.

When registering the domain names, this must have been obvious to the Respondent, as the Complainant is also famous in the UK. It is likely that the Respondent is familiar with football, as he has several other football domains, but even if this was not the case it would be likely that he knew about the Complainant and the Complainant’s trademarks.

The Panel finds that the Respondent intentionally attempted to attract, for commercial gain, Internet users to the Respondent’s web site by creating a likelihood of confusion with the Complainant’s mark and name as to the sponsorship, affiliation, or endorsement of the Respondent’s web site or the services constituting the Respondent’s business activities.

The Panel finds that the domain names were registered and used in bad faith.

7. Decision

For all the foregoing reasons, in accordance with Paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the domain names, <bayernmunchen.net> and <bayernmuenchen.net> be transferred to the Complainant.

Peter G. Nitter
Sole Panelist

Dated: July 15, 2003

Dr. Michael Crichton v. In Stealth Mode Case No: D2002-0074
Statement of Acceptance and Declaration of Impartiality and Independence, as required by the Center to ensure compliance with the Rules, paragraph 7.

The language of the proceeding was English, being the language of the registration agreement.

4. Factual Background (uncontested facts)

Complainant is a well-known author and director who has published numerous books, screenplays and other works under his own name. These include:

Novels:

Non-fiction Books:

Motion Pictures:

Television:
"ER", broadcast from 1994 through the present.

Respondent registered the disputed domain name on June 4, 2002. It connects Internauts to Respondent's <ebuzz.com> website, which carries nothing about Complainant or his works but advertises commercial services, such as its "matchmaker" and messaging services.

Respondent is not, and has never been, personally or professionally known as Michael Crichton. Respondent does not transact in goods or services related to Michael Crichton, and is not otherwise authorized or permitted to use the name Michael Crichton. Complainant contacted Respondent requesting the transfer of the disputed domain name, but Respondent failed to reply.

5. Parties’ Contentions

A. Complainant

Complainant's name has become a famous common law trademark. The disputed domain name is identical to the mark. Respondent has no rights or legitimate interests in the disputed domain name, which was registered and is being used in bad faith.

B. Respondent

The Respondent did not reply to the Complainant's contentions.

6. Discussion and Findings

Under paragraph 15(a) of the Rules, the Panel must decide this Complaint on the basis of the statements and documents submitted and in accordance with the Policy, the Rules and any rules and principles of law that it deems applicable.

To qualify for cancellation or transfer, a Complainant must prove each element of paragraph 4(a) of the Policy, namely:

(i) the disputed domain name is identical or confusingly similar to a trademark or service mark in which Complainant has rights; and

(ii) Respondent has no rights or legitimate interests in respect of the domain name; and

(iii) the disputed domain name has been registered and is being used in bad faith.

Failure to File a Response

A respondent is not obliged to participate in a domain name dispute proceeding, but if it were to fail to do so, asserted facts that are not unreasonable would be taken as true and the respondent would be subject to the inferences that flow naturally from the information provided by the complainant: Reuters Limited v. Global Net 2000, Inc., WIPO Case No. D2000-0441. See also Hewlett-Packard Company v. Full System, NAF Case No. FA-0094637; David G. Cook v. This Domain is For Sale, NAF Case No. FA0094957 and Gorstew Jamaica and Unique Vacations, Inc. v. Travel Concierge, NAF Case No. FA0094925.

A. Identical or Confusingly Similar

In light of the Second WIPO Domain Name Process, it is clear that the Policy is not intended to apply to personal names that have not been used commercially and acquired secondary meaning as the source of goods and/or services, i.e. common law trademark rights: The Reverend Dr. Jerry Falwell and The Liberty Alliance v. Gary Cohn, Prolifec.net and God.info, WIPO Case No. D2002-0184; Israel Harold Asper v. Communication X Inc., WIPO Case No. D2001-0540; Kathleen Kennedy Townsend v. B. G. Birt, WIPO Case No. D2002-0053; RE'Ted Turner and Ted Turner Film Properties, LLC v. Mazen Fahmi, WIPO Case No. D2002-0251.

To establish common law rights in a personal name, it is necessary to show use of that name as an indication of the source of goods or services supplied in trade or commerce and that, as a result of such use, the name has become distinctive of that source. Upon such proof, a celebrity's name can serve as a trademark when used to identify the celebrity's performance services: Kevin Spacey v. Alberta Hot Rods, NAF Case No. FA0205000114437.

Complainant has claimed to be the author of the numerous works already identified. Respondent has not contested this. The Panel therefore infers that Complainant has, through use, acquired common law trademark rights in his name. The Panel finds the disputed domain name is identical to Complainant's mark. Complainant has established this element of his case.

B. Rights or Legitimate Interests

Likewise, in the absence of a Response, the Panel accepts that Respondent is not known by the disputed domain name, does not transact in goods or services related to Complainant and is not authorized by Complainant to use his mark. These
circumstances are sufficient to constitute a prima facie showing by Complainant of absence of rights or legitimate interests in the disputed domain name on the part of Respondent. The evidentiary burden, therefore, shifts to Respondent to show that it does have rights or legitimate interests in the domain name, whether by reference to the examples set out in paragraph 4(c) of the Policy or otherwise:

Do The Hustle, LLC v. Tropic Web, WIPO Case No. D2000-0624 and the cases there cited. Respondent has made no such showing.

Internet users who access the disputed domain name are automatically transported to Respondent’s commercial website at <ebuzz.com>. In similar circumstances, the Panel in Stephanie Seymour v. Jeff Burgar d/b/a Stephanie Seymour Club, NAF Case No. FA010400097112 held that by virtue of serving only as a portal, such a website “evidences no bona fide authorized offering of goods and services whatsoever and does nothing but misappropriate Complainant’s trademark in order to lure Internet users to Respondent’s commercial site”. Likewise in Michael Andretti v. Alberta Hot Rods, NAF Case No. FA0108000099084.

Here, as in Stephanie Seymour and Michael Andretti, Complainant’s name is well-known as a trademark. Accordingly, Respondent’s unauthorized use of the disputed domain name to lead to the <ebuzz.com> site cannot be accepted as bona fide use.

1. The Parties

The Panel finds Respondent has no rights or legitimate interest in the disputed domain name. Complainant has established this element of its case.

C. Registered and Used in Bad Faith

Internauts entering a domain name of a celebrity famously associated in commerce with the supply of goods or services expect to find a site offering goods or services associated with the celebrity’s trademark. Here they find a site that has no association with Complainant or his mark. It follows that the Panel finds Respondent has used the disputed domain name intentionally to attempt to attract, for commercial gain, Internauts to its website by creating a likelihood of confusion with Complainant’s mark as to the source, sponsorship, affiliation or endorsement of its website. Under paragraph 4(c)(iv) of the Policy, this shall be evidence of both bad faith registration and use.

7. Decision

For all the foregoing reasons, in accordance with paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the domain name <michael-crichton.com> be transferred to Complainant.


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

Whereas:

(1) The content of Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (3) has been amended (4). In the interests of clarity and rationality the said Directive should be codified.

(2) The trade mark laws applicable in the Member States before the entry into force of Directive 89/104/EEC contained disparities which may have impeded the free movement of goods and freedom to provide services and may have distorted competition within the common market. It was therefore necessary to approximate the laws of the Member States in order to ensure the proper functioning of the internal market.

(3) It is important not to disregard the solutions and advantages which the Community trade mark system may afford to undertakings wishing to acquire trade marks.

(4) It does not appear to be necessary to undertake full-scale approximation of the trade mark laws of the Member States. It will be sufficient if approximation is limited to those national provisions of law which most directly affect the functioning of the internal market.

(5) This Directive should not deprive the Member States of the right to continue to protect trade marks acquired through use but should take them into account only in regard to the relationship between them and trade marks acquired by registration.

(6) Member States should also remain free to fix the provisions of procedure concerning the registration, the revocation and the invalidity of trade marks acquired by registration. They can, for example, determine the form of trade mark registration and invalidity procedures, decide whether earlier rights should be invoked either in the registration procedure or in the invalidity procedure or in both and, if they allow earlier rights to be invoked in the registration procedure, have an opposition procedure or an ex officio examination procedure or both. Member States should remain free to determine the effects of revocation or invalidity of trade marks.

(7) This Directive should not exclude the application to trade marks of provisions of law of the Member States other than trade mark law, such as the provisions relating to unfair competition, civil liability or consumer protection.

(8) Attainment of the objectives at which this approximation of laws is aiming requires that the conditions for obtaining and continuing to hold a registered trade mark be, in general, identical in all Member States. To this end, it is necessary to list examples of signs which may constitute a trade mark, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other
undertakings. The grounds for refusal or invalidity concerning the trade mark itself, for example, the absence of any distinctive character, or concerning conflicts between the trade mark and earlier rights, should be listed in an exhaustive manner, even if some of these grounds are listed as an option for the Member States which should therefore be able to maintain or introduce those grounds in their legislation. Member States should be able to maintain or introduce into their legislation grounds of refusal or invalidity linked to conditions for obtaining and continuing to hold a trade mark for which there is no provision of approximation, concerning, for example, the eligibility for the grant of a trade mark, the renewal of the trade mark or rules on fees, or related to the non-compliance with procedural rules.

(9) In order to reduce the total number of trade marks registered and protected in the Community and, consequently, the number of conflicts which arise between them, it is essential to require that registered trade marks must actually be used or, if not used, be subject to revocation. It is necessary to provide that a trade mark cannot be invalidated on the basis of the existence of a non-used earlier trade mark, while the Member States should remain free to apply the same principle in respect of the registration of a trade mark or to provide that a trade mark may not be successfully invoked in infringement proceedings if it is established as a result of a plea that the trade mark could be revoked. In these cases it is up to the Member States to establish the applicable rules of procedure.

(10) It is fundamental, in order to facilitate the free movement of goods and services, to ensure that registered trade marks enjoy the same protection under the legal systems of all the Member States. This should not, however, prevent the Member States from granting at their option extensive protection to their trade marks which have a reputation.

(11) The protection afforded by the registered trade mark, the function of which is in particular to guarantee the trade mark as an indication of origin, should be absolute in the case of identity between the mark and the sign and the goods or services. The protection should apply also in the case of similarity between the mark and the sign and the goods or services. It is indispensable to give an interpretation of the concept of similarity in relation to the likelihood of confusion. The likelihood of confusion, the appreciation of which depends on numerous elements and, in particular, on the recognition of the trade mark on the market, the association which can be made with the used or registered sign, the degree of similarity between the trade mark and the sign and between the goods or services identified, should constitute the specific condition for such protection. The ways in which likelihood of confusion may be established, and in particular the onus of proof should be a matter for national procedural rules which should not be prejudiced by this Directive.

(12) It is important, for reasons of legal certainty and without inequitably prejudicing the interests of a proprietor of an earlier trade mark, to provide that the latter may no longer request a declaration of invalidity nor may he oppose the use of a trade mark subsequent to his own of which he has knowingly tolerated the use for a substantial length of time, unless the application for the subsequent trade mark was made in bad faith.

(13) All Member States are bound by the Paris Convention for the Protection of Industrial Property. It is necessary that the provisions of this Directive should be entirely consistent with those of the said Convention. The obligations of the Member States resulting from that Convention should not be affected by this Directive. Where appropriate, the second paragraph of Article 307 of the Treaty should apply.

(14) This Directive should be without prejudice to the obligations of the Member States relating to the time limit for transposition into national law of Directive 89/104/EEC set out in Annex I, Part B.

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope
This Directive shall apply to every trade mark in respect of goods or services which is the subject of registration or of an application in a Member State for registration as an individual trade mark, a collective mark or a guarantee or certification mark, or which is the subject of a registration or an application for registration in the Benelux Office for Intellectual Property or of an international registration having effect in a Member State.

Article 2
Signs of which a trade mark may consist
A trade mark may consist of any signs capable of being represented graphically, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings.

Article 3
Grounds for refusal or invalidity
1. The following shall not be registered or, if registered, shall be liable to be declared invalid:
   (a) signs which cannot constitute a trade mark;
   (b) trade marks which are devoid of any distinctive character;
   (c) trade marks which consist exclusively of signs or indications which may serve, in trade, to designate the kind, quantity, intended purpose, value, geographical origin, or the time of production of the goods or of rendering of the service, or other characteristics of the goods or services;
   (d) trade marks which consist exclusively of signs or indications which have become customary in the current language or in the bona fide and established practices of the trade;
   (e) signs which consist exclusively of:
      (i) the shape which results from the nature of the goods themselves;
      (ii) the shape of goods which is necessary to obtain a technical result;
      (iii) the shape which gives substantial value to the goods;
   (f) trade marks which are contrary to public policy or to accepted principles of morality;
   (g) trade marks which are of such a nature as to deceive the public, for instance as to the nature, quality or geographical origin of the goods or service;
   (h) trade marks which have not been authorised by the competent authorities and are to be refused or invalided pursuant to Article 6 ter of the Paris Convention for the Protection of Industrial Property, hereinafter referred to as the 'Paris Convention'.
2. Any Member State may provide that a trade mark shall not be registered or, if registered, shall be liable to be declared invalid where and to the extent that:
   (a) the use of that trade mark may be prohibited pursuant to provisions of law other than trade mark law of the Member State concerned or of the Community;
   (b) the trade mark covers a sign of high symbolic value, in particular a religious symbol;
   (c) the trade mark includes badges, emblems and escutcheons other than those covered by Article 6 ter of the Paris Convention and which are of public interest, unless the consent of the competent authority to their registration has been given in conformity with the legislation of the Member State;
   (d) the application for registration of the trade mark was made in bad faith by the applicant.
3. A trade mark shall not be refused registration or be declared invalid in accordance with paragraph 1(b), (c) or (d) if, before the date of application for registration and following the use which has been made of it, it has acquired a distinctive character. Any Member State may in addition provide that this provision shall also apply where the distinctive character was acquired after the date of application for registration or after the date of registration.

4. Any Member State may provide that, by derogation from paragraphs 1, 2 and 3, the grounds of refusal of registration or invalidity in force in that State prior to the date of entry into force of the provisions necessary to comply with Directive 89/104/EEC, shall apply to trade marks for which application has been made prior to that date.

Article 4
Further grounds for refusal or invalidity concerning conflicts with earlier rights

1. A trade mark shall not be registered or, if registered, shall be liable to be declared invalid:
   (a) if it is identical with an earlier trade mark, and the goods or services for which the trade mark is applied for or is registered are identical with the goods or services for which the earlier trade mark is protected;
   (b) if because of its identity with, or similarity to, the earlier trade mark and the identity or similarity of the goods or services covered by the trade marks, there exists a likelihood of confusion on the part of the public; the likelihood of confusion includes the likelihood of association with the earlier trade mark.

2. Earlier trade marks' within the meaning of paragraph 1 means:
   (a) trade marks of the following kinds with a date of application for registration which is earlier than the date of application for registration of the trade mark, taking account, where appropriate, of the priorities claimed in respect of those trade marks;
   (i) Community trade marks;
   (ii) trade marks registered in the Member State or, in the case of Belgium, Luxembourg or the Netherlands, at the Benelux Office for Intellectual Property;
   (iii) trade marks registered under international arrangements which have effect in the Member State;
   (b) Community trade marks which validly claim seniority, in accordance with Council Regulation (EC) No 40/94 (5) of 20 December 1993 on the Community trade mark, from a trade mark referred to in (a)(i) and (ii), even when the latter trade mark has been surrendered or allowed to lapse;
   (c) applications for the trade marks referred to in points (a) and (b), subject to their registration;
   (d) trade marks which, on the date of application for registration of the trade mark, or, where appropriate, of the priority claimed in respect of the application for registration of the trade mark, are well known in a Member State, in the sense in which the words 'well known' are used in Article 6 bis of the Paris Convention.

3. A trade mark shall furthermore not be registered or, if registered, shall be liable to be declared invalid if it is identical with, or similar to, an earlier Community trade mark within the meaning of paragraph 2 and is to be, or has been, registered for goods or services which are not similar to those for which the earlier Community trade mark is registered, and where the earlier Community trade mark has a reputation in the Community and where the use of the later trade mark without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the reputation of the earlier Community trade mark.

4. Any Member State may, in addition, provide that a trade mark shall not be registered or, if registered, shall be liable to be declared invalid where, and to the extent that:
   (a) the trade mark is identical with, or similar to, an earlier national trade mark within the meaning of paragraph 2 and is to be, or has been, registered for goods or services which are not similar to those for which the earlier trade mark is registered, where the earlier trade mark has a reputation in the Member State concerned and where the use of the later trade mark without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the reputation of the earlier trade mark;
   (b) to a right to a name;
   (ii) a right of personal portrayal;
   (iii) a copyright;
   (iv) an industrial property right;
   (d) the trade mark is identical with, or similar to, an earlier collective trade mark conferring on a right which registered on a period of a maximum of three years preceding application;
   (e) the trade mark is identical with, or similar to, an earlier guarantee or certification mark conferring a right which expired within a period preceding application the length of which is fixed by the Member State;
   (f) the trade mark is identical with, or similar to, an earlier trade mark which was registered for identical or similar goods or services and conferred on them a right which has expired for failure to renew within a period of a maximum of two years preceding application, unless the proprietor of the earlier trade mark gave his agreement for the registration of the later mark or did not use his trade mark;
   (g) the trade mark is liable to be confused with a mark which was in use abroad on the filing date of the application and which is still in use there, provided that at the date of the application the applicant was acting in bad faith.

5. The Member States may permit that in appropriate circumstances registration need not be refused or the trade mark need not be declared invalid where the proprietor of the earlier trade mark or other earlier right consents to the registration of the later trade mark.

6. Any Member State may provide that, by derogation from paragraphs 1 to 5, the grounds for refusal of registration or invalidity in force in that State prior to the date of the entry into force of the provisions necessary to comply with Directive 89/104/EEC, shall apply to trade marks for which application has been made prior to that date.

Article 5
Rights conferred by a trade mark

1. The registered trade mark shall confer on the proprietor exclusive rights therein. The proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade:
   (a) any sign which is identical with the trade mark in relation to goods or services which are identical with those for which the trade mark is registered;
   (b) any sign where, because of its identity with, or similarity to, the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, there exists a likelihood of confusion between the sign and the trade mark.

2. Any Member State may also provide that the proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade any sign which is identical with, or similar to, the trade mark in relation to goods or services which are not identical with those for which the trade mark is registered, where the latter has a reputation in the Member State and where use of that sign without due cause takes unfair advantage of, or is
detrimental to, the distinctive character or the repute of the trade mark.

3. The following, inter alia, may be prohibited under paragraphs 1 and 2:
(a) affixing the sign to the goods or to the packaging thereof;
(b) offering the goods, or putting them on the market or stocking them for these purposes under that sign, or offering or supplying services thereunder;
(c) importing or exporting the goods under the sign;
(d) using the sign on business papers and in advertising.

4. Where, under the law of the Member State, the use of a sign under the conditions referred to in paragraph 1(b) or paragraph 2 could not be prohibited before the date of entry into force of the provisions necessary to comply with Directive 89/104/EEC in the Member State concerned, the rights conferred by the trade mark may not be relied on to prevent the continued use of the sign.

5. Paragraphs 1 to 4 shall not affect provisions in any Member State relating to the protection against the use of a sign other than for the purposes of distinguishing goods or services, where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark.

Article 6
Limitation of the effects of a trade mark
1. The trade mark shall not entitle the proprietor to prohibit a third party from using, in the course of trade:
(a) his own name or address;
(b) indications concerning the kind, quality, quantity, intended purpose, value, geographical origin, the time of production of goods or of rendering of the service, or other characteristics of goods or services;
(c) the trade mark where it is necessary to indicate the intended purpose of a product or service, in particular as accessories or spare parts;

provided he uses them in accordance with honest practices in industrial or commercial matters.

2. The trade mark shall not entitle the proprietor to prohibit a third party from using, in the course of trade, an earlier right which only applies in a particular locality if that right is recognised by the laws of the Member State in question and within the limits of the territory in which it is recognised.

Article 7
Exhaustion of the rights conferred by a trade mark
1. The trade mark shall not entitle the proprietor to prohibit its use in relation to goods which have been put on the market in the Community under that trade mark by the proprietor or with his consent.

2. Paragraph 1 shall not apply where there exist legitimate reasons for the proprietor to oppose further commercialisation of the goods, especially where the condition of the goods is changed or impaired after they have been put on the market.

Article 8
Licensing
1. A trade mark may be licensed for some or all of the goods or services for which it is registered and for the whole or part of the Member State concerned. A licence may be exclusive or non-exclusive.

2. The proprietor of a trade mark may invoke the rights conferred by that trade mark against a licensee who contravenes any provision in his licensing contract with regard to:
(a) its duration;
(b) the form covered by the registration in which the trade mark may be used;
(c) the scope of the goods or services for which the licence is granted;
(d) the territory in which the trade mark may be affixed; or
(e) the quality of the goods manufactured or of the services provided by the licensee.

Article 9
Limitation in consequence of acquiescence
1. Where, in a Member State, the proprietor of an earlier trade mark as referred to in Article 4(2) has acquiesced, for a period of five successive years, in the use of a later trade mark registered in that Member State while being aware of such use, he shall no longer be entitled on the basis of the earlier trade mark either to apply for a declaration that the later trade mark is invalid or to oppose the use of the later trade mark in respect of the goods or services for which the later trade mark has been used, unless registration of the later trade mark was applied for in bad faith.

2. Any Member State may provide that paragraph 1 shall apply mutatis mutandis to the proprietor of an earlier trade mark referred to in Article 4(4)(a) or an other earlier right referred to in Article 4(4)(b) or (c).

3. In the cases referred to in paragraphs 1 and 2, the proprietor of a later registered trade mark shall not be entitled to oppose the use of the earlier right, even though that right may no longer be invoked against the later trade mark.

Article 10
Use of trade marks
1. If, within a period of five years following the date of the completion of the registration procedure, the proprietor has not put the trade mark to genuine use in the Member State in connection with the goods or services in respect of which it is registered, or if such use has been suspended during an uninterrupted period of five years, the trade mark shall be subject to the sanctions provided for in this Directive, unless there are proper reasons for non-use.

The following shall also constitute use within the meaning of the first subparagraph:
(a) use of the trade mark in a form differing in elements which do not alter the distinctive character of the mark in the form in which it was registered;
(b) affixing of the trade mark to goods or to the packaging thereof in the Member State concerned solely for export purposes.

2. Use of the trade mark with the consent of the proprietor or by any person who has authority to use a collective mark or a guarantee or certification mark shall be deemed to constitute use by the proprietor.

3. In relation to trade marks registered before the date of entry into force in the Member State concerned of the provisions necessary to comply with Directive 89/104/EEC:
(a) where a provision in force prior to that date attached sanctions to non-use of a trade mark during an uninterrupted period, the relevant period of five years mentioned in the first subparagraph of paragraph 1 shall be deemed to have begun to run at the same time as any period of non-use which is already running at that date;
(b) where there was no use provision in force prior to that date, the periods of five years mentioned in the first subparagraph of paragraph 1 shall be deemed to run from that date at the earliest.

Article 11
Sanctions for non-use of a trade mark in legal or administrative proceedings
1. A trade mark may not be declared invalid on the ground that there is an earlier conflicting trade mark if the latter does not fulfill the requirements of use set out in Article 10(1) and (2), or in Article 10(3), as the case may be.

2. Any Member State may provide that registration of a trade mark may not be refused on the ground that there is an earlier conflicting trade mark if the latter does not fulfill the requirements of use set out in Article 10(1) and (2) or in Article 10(3), as the case may be.

3. Without prejudice to the application of Article 12, where a counter-claim for revocation is made, any Member State may provide that a trade mark may not be successfully invoked in infringement proceedings if it is established as a result of a
plea that the trade mark could be revoked pursuant to Article 12(1).

4. If the earlier trade mark has been used in relation to part only of the goods or services for which it is registered, it shall, for purposes of applying paragraphs 1, 2 and 3, be deemed to be registered in respect only of that part of the goods or services.

Article 12

Grounds for revocation

1. A trade mark shall be liable to revocation if, within a continuous period of five years, it has not been put to genuine use in the Member State in connection with the goods or services in respect of which it is registered, and there are no proper reasons for non-use.

However, no person may claim that the proprietor's rights in a trade mark should be revoked where, during the interval between expiry of the five-year period and filing of the application for revocation, genuine use of the trade mark has been started or resumed.

The commencement or resumption of use within a period of three months preceding the filing of the application for revocation which began at the earliest on expiry of the continuous period of five years of non-use shall be disregarded where preparations for the commencement or resumption occur only after the proprietor becomes aware that the application for revocation may be filed.

2. Without prejudice to paragraph 1, a trade mark shall be liable to revocation if, after the date on which it was registered:

(a) in consequence of acts or inactivity of the proprietor, it has become the common name in the trade for a product or service in respect of which it is registered;

(b) in consequence of the use made of it by the proprietor of the trade mark or with his consent in respect of the goods or services for which it is registered, it is liable to mislead the public, particularly as to the nature, quality or geographical origin of those goods or services.

Article 13

Grounds for refusal or revocation or invalidity relating to only some of the goods or services

Where grounds for refusal of registration or for revocation or invalidity of a trade mark exist in respect of only some of the goods or services for which that trade mark has been applied for or registered, refusal of registration or revocation or invalidity shall cover those goods or services only.

Article 14

Establishment a posteriori of invalidity or revocation of a trade mark

Where the seniority of an earlier trade mark which has been surrendered or allowed to lapse is claimed for a Community trade mark, the invalidity or revocation of the earlier trade mark may be established a posteriori.

Article 15

Special provisions in respect of collective marks, guarantee marks and certification marks

1. Without prejudice to Article 4, Member States whose laws authorise the registration of collective marks or of guarantee or certification marks may provide that such marks shall not be registered, or shall be revoked or declared invalid, on grounds additional to those specified in Articles 3 and 12 where the function of those marks so requires.

2. By way of derogation from Article 3(1)(c), Member States may provide that signs or indications which may serve, in trade, to designate the geographical origin of the goods or services may constitute collective, guarantee or certification marks. Such a mark does not entitle the proprietor to prohibit a third party from using in the course of trade such signs or indications, provided he uses them in accordance with honest practices in industrial or commercial matters; in particular, such a mark may not be invoked against a third party who is entitled to use a geographical name.

Article 16

Communication

Member States shall communicate to the Commission the text of the main provisions of national law adopted in the field governed by this Directive.

Article 17

Repeal

Directive 89/104/EEC, as amended by the Decision listed in Annex I, Part A, is repealed, without prejudice to the obligations of the Member States relating to the time limit for transposition into national law of that Directive, set out in Annex I, Part B.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex II.

Article 18

Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 19

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 22 October 2008.

For the European Parliament

The President

H.-G. PÖTTERING

For the Council

The President

J.-P. JOUYET

(1) OJ C 161, 13.7.2007, p. 44.


(4) See Annex I, Part A.

Regulation (EC) No 733/2002 of the European Parliament and of the council of 22 April 2002 on the implementation of the .eu Top Level Domain

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 156 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Following consultation of the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) The creation of the .eu Top Level Domain (TLD) is included as one of the targets to accelerate electronic commerce in the e-Europe initiative as endorsed by the European Council at its meeting in Lisbon on 23 and 24 March 2000.

(2) The communication from the Commission to the Council and the European Parliament on the organisation and management of the Internet refers to the creation of the .eu TLD and the Council resolution of 3 October 2000 on the organisation and management of the Internet (4) charges the Commission to encourage the coordination of policies in relation to the management of the Internet.

(3) TLDs are an integral part of the Internet infrastructure. They are an essential element of the global interoperability of the World Wide Web ("WWW" or "the Web"). The connection and presence permitted by the allocation of domain names and the related addresses allow users to locate computers and websites on the Web. TLDs are also an integral part of every Internet e-mail address.

(4) The .eu TLD should promote the use of, and access to, the Internet networks and the virtual market place based on the Internet, in accordance with Article 154(2) of the Treaty, by providing a complementary registration domain to existing country code Top Level Domains (ccTLDs) or global registration in the generic Top Level Domains, and should in consequence increase choice and competition.

(5) The .eu TLD should improve the interoperability of trans-European networks, in accordance with Articles 154 and 155 of the Treaty, by ensuring the availability of .eu name servers in the Community. This will affect the topology and technical infrastructure of the Internet in Europe which will benefit from an additional set of name servers in the Community.

(6) Through the .eu TLD, the internal market should acquire higher visibility in the virtual market place based on the Internet. The .eu TLD should provide a clearly identified link with the Community, the associated legal framework, and the European market place. It should enable undertakings, organisations and natural persons within the Community to register in a specific domain which will make this link obvious. As such, the .eu TLD will not only be a key building block for electronic commerce in Europe but will also support the objectives of Article 14 of the Treaty.

(7) The .eu TLD can accelerate the benefits of the information society in Europe as a whole, play a role in the integration of future Member States into the European Union, and help combat the risk of digital divide with neighbouring countries. It is therefore to be expected that this Regulation will be extended to the European Economic Area and that amendments may be sought to the existing arrangements between the European Union and European third countries, with a view to accommodating the requirements of the .eu TLD so that entities in those countries may participate in it.

(8) This Regulation is without prejudice to Community law in the field of personal data protection. This Regulation should be implemented in compliance with the principles relating to privacy and the protection of personal data.

(9) Internet management has generally been based on the principles of non-interference, self-management and self-regulation. To the extent possible and without prejudice to Community law, these principles should also apply to the .eu ccTLD. The implementation of the .eu TLD may take into consideration best practices in this regard and could be supported by voluntary guidelines or codes of conduct where appropriate.

(10) The establishment of the .eu TLD should contribute to the promotion of the European Union image on the global information networks and bring an added value to the Internet naming system in addition to the national ccTLDs.

(11) The objective of this Regulation is to establish the conditions of implementation of the .eu TLD, to provide for the designation of a Registry and establish the general policy framework within which the Registry will function. National ccTLDs are not covered by this Regulation.

(12) The Registry is the entity charged with the organisation, administration and management of the .eu TLD, including maintenance of the corresponding databases and the associated public query services, the accreditation of Registrars, the registration of domain names applied for by accredited Registrars, the operation of the TLD name servers and the dissemination of TLD zone files. Public query services associated with the TLD are referred to as 'Who is' queries. Who is-type databases should be in conformity with Community law on data protection and privacy. Access to these databases provides information on a domain name holder and is an essential tool in boosting user confidence.

(13) After publishing a call for expressions of interest in the Official Journal of the European Communities, the Commission should, on the basis of an open, transparent and non-discriminatory selection procedure, designate a Registry. The Commission
should enter into a contract with the selected Registry which should specify the conditions applying to the Registry for the organisation, administration and management of the .eu TLD and which should be limited in time and renewable.

(14) The Commission, acting on behalf of the Community, has requested the delegation of the EU code for the purpose of creating an Internet ccTLD. On 25 September 2000, the Internet Corporation for Assigned Names and Numbers (ICANN) issued a resolution providing that ‘alpha-2 codes are delegable as ccTLDs only in cases where the ISO 3166 Maintenance Agency, on its exceptional reservation list, has issued a reservation of the code that covers any application of ISO 3166-1 that needs a coded representation in the name of the country, territory or area involved’. Such conditions are met by the EU code which is therefore ‘delegable’ to the Community.

(15) ICANN is at present responsible for coordinating the delegation of codes representing ccTLD to Registries. The Council resolution of 3 October 2000 encourages the implementation of the principles applied to ccTLD Registries adopted by the Governmental Advisory Committee (GAC). The Registry should enter into a contract with ICANN respecting the GAC principles.

(16) The adoption of a public policy addressing speculative and abusive registration of domain names should provide that holders of prior rights recognised or established by national and/or Community law and public bodies will benefit from a specific period of time (a ‘sunset period’) during which the registration of their domain names is exclusively reserved to such holders of prior rights recognised or established by national and/or Community law and public bodies.

(17) Domain names should not be revoked arbitrarily. A revocation may, however, be obtained in particular should a domain name be manifestly contrary to public order. The revocation policy should nevertheless provide for a timely and efficient mechanism.

(18) Rules should be adopted on the question of bona vacantia to address the status of domain names the registration of which is not renewed or which, for example because of succession law, are left without holder.

(19) The new .eu TLD registry should not be empowered to create second-level domains using alpha-2 codes representing countries.

(20) Within the framework established by this Regulation, the public policy rules concerning the implementation and functions of the .eu TLD and the public policy principles on registration, various options including the ‘first come, first served’ method should be considered when registration policy is formulated.

(21) When reference is made to interested parties, provision should be made for consultation encompassing, in particular, public authorities, undertakings, organisations and natural persons. The Registry could establish an advisory body to organise such consultation.

(22) The measures necessary for the implementation of this Regulation, including criteria for the selection procedure of the Registry, the designation of the Registry, as well as the adoption of public policy rules, should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (5).

(23) Since the objective of the proposed action, namely to implement the .eu TLD, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

HAVE ADOPTED THIS REGULATION:

Article 1

Objective and scope

1. The objective of this Regulation is to implement the .eu country code Top Level Domain (ccTLD) within the Community. The Regulation sets out the conditions for such implementation, including the designation of a Registry, and establishes the general policy framework within which the Registry will function.

2. This Regulation shall apply without prejudice to arrangements in Member States regarding national ccTLDs.

Article 2

Definitions

For the purposes of this Regulation:

(a) ‘Registry’ means the entity entrusted with the organisation, administration and management of the .eu TLD, including maintenance of the corresponding databases and the associated public query services, registration of domain names, operation of the Registry of domain names, operation of the Registry TLD name servers and dissemination of TLD zone files;

(b) ‘Registrar’ means a person or entity that, via contract with the Registry, provides domain name registration services to registrants.

Article 3

Characteristics of the Registry

1. The Commission shall:

(1) establish the criteria and the procedure for the designation of the Registry. That measure, designed to amend non-essential elements of this Regulation by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 6(3). On imperative grounds of urgency, the Commission may have recourse to the urgency procedure referred to in Article 6(4);

(2) designate, in accordance with the procedure referred to in Article 6(2), the Registry after publishing a call for expressions of interest in the Official Journal of the European Communities and after the procedure for such call has been completed;

(c) enter into, in accordance with the procedure referred to in Article 6(2), a contract which shall specify the conditions according to which the Commission supervises the organisation, administration and management of the .eu TLD by the Registry. The contract between the Commission and the Registry shall be limited in time and renewable. The Registry may not accept registrations until the registration policy is in place.
2. The Registry shall be a non-profit organisation, formed in accordance with the law of a Member State and having its registered office, central administration and principal place of business within the Community.

3. Having obtained the prior consent of the Commission, the Registry shall enter into the appropriate contract providing for the delegation of the .eu ccTLD code. To this effect the relevant principles adopted by the Governmental Advisory Committee shall be taken into account.

4. The .eu TLD Registry shall not act itself as Registrar.

Article 4

Obligations of the Registry

1. The Registry shall observe the rules, policies and procedures laid down in this Regulation and the contracts referred to in Article 3. The Registry shall observe transparent and non-discriminatory procedures.

2. The Registry shall:
   (a) organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality, efficiency, reliability and accessibility;
   (b) register domain names in the .eu TLD through any accredited .eu Registrar requested by any:
      (i) undertaking having its registered office, central administration or principal place of business within the Community, or
      (ii) organisation established within the Community without prejudice to the application of national law, or
      (iii) natural person resident within the Community;
   (c) impose fees directly related to costs incurred;
   (d) implement the extra-judicial settlement of conflicts policy based on recovery of costs and a procedure to resolve promptly disputes between domain name holders regarding rights relating to names including intellectual property rights as well as disputes in relation to individual decisions by the Registry. This policy shall be adopted in accordance with Article 5(1) and take into consideration the recommendations of the World Intellectual Property Organisation. The policy shall provide adequate procedural guarantees for the parties concerned, and shall apply without prejudice to any court proceeding;
   (e) adopt procedures for, and carry out, accreditation of .eu Registrars and ensure effective and fair conditions of competition among .eu Registrars;
   (f) ensure the integrity of the databases of domain names.

Article 5

Policy framework

1. After consulting the Registry, the Commission shall adopt public policy rules concerning the implementation and function of the .eu TLD and public policy principles on registration. Those measures, designed to amend non-essential elements of this Regulation by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 6(3).

   1. Public policy shall include:
      (a) an extra-judicial settlement of conflicts policy;
      (b) public policy on speculative and abusive registration of domain names, including the possibility of registration of domain names in a phased manner to ensure appropriate temporary opportunities for the holders of prior rights recognised or established by national and/or Community law and public bodies to register their names;
      (c) policy on possible revocation of domain names, including the question of bona vacantia;
      (d) issues of language and geographical concepts;
      (e) treatment of intellectual property and other rights.

2. Within three months of the entry into force of this Regulation, Member States may notify to the Commission and to the other Member States a limited list of broadly-recognised names with regard to geographical and/or geopolitical concepts which affect their political or territorial organisation that may either:
   (a) not be registered, or
   (b) be registered only under a second level domain according to the public policy rules.

The Commission shall notify to the Registry without delay the list of notified names to which such criteria apply. The Commission shall publish the list at the same time as it notifies the Registry.

Where a Member State or the Commission within 30 days of publication raises an objection to an item included in a notified list, the Commission shall take measures, in accordance with the procedure referred to in Article 6(3), to remedy the situation.

3. Before starting registration operations, the Registry shall adopt the initial registration policy for the .eu TLD in consultation with the Commission and other interested parties. The Registry shall implement in the registration policy the public policy rules adopted pursuant to paragraph 1 taking into account the exception lists referred to in paragraph 2.

4. The Commission shall periodically inform the Committee referred to in Article 6 on the activities referred to in paragraph 3 of this Article.

Article 6

Committee procedure


2. Where reference is made to this paragraph, Articles 3 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

4. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

Article 7

Reservation of rights

The Community shall retain all rights relating to the .eu TLD including, in particular, intellectual property rights and other rights to the Registry databases required to ensure the implementation of this Regulation and the right to re-designate the Registry.

Article 8

Implementation report

The Commission shall submit a report to the European Parliament and the Council on the implementation, effectiveness and functioning of the .eu TLD one year after the adoption of this Regulation and thereafter every two years.

Article 9

Entry into force

This Regulation shall enter into force on the day of its publication in the Official Journal of the European Communities. This Regulation shall be binding in its entirety and directly applicable in all Member States.

(1) OJ C 96 E, 27.3.2001, p. 333.
(2) OJ C 155, 29.5.2001, p. 10.
Amended by:


Commission regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration

(Text with EEA relevance)

COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (1), and in particular Article 5(1) thereof,

Having consulted the Registry in accordance with Article 5(1) of Regulation (EC) No 733/2002,

Whereas:

(1) The initial implementation stages of the .eu Top Level Domain (TLD), to be created pursuant to Regulation (EC) No 733/2002, have been completed by designating a legal entity, established within the Community to administer and manage the .eu TLD Registry function. The Registry, designated by Commission Decision 2003/375/EC (2), is required to be a non-profit organisation that should operate and provide services on a cost covering basis and at an affordable price.

(2) Requesting a domain name should be possible through electronic means in a simple, speedy and efficient procedure, in all official languages of the Community, through accredited registrars.

(3) Accreditation of registrars should be carried out by the Registry following a procedure that ensures fair and open competition between Registrars. The accreditation process should be objective, transparent and non-discriminatory. Only parties who meet certain basic technical requirements to be determined by the Registry should be eligible for accreditation.

(4) Registrars should only accept applications for the registration of domain names filed after their accreditation and should forward them in the chronological order in which they were received.

(5) To ensure better protection of consumers' rights, and without prejudice to any Community rules concerning jurisdiction and applicable law, the applicable law in disputes between registrars and registrants on matters concerning Community titles should be the law of one of the Member States.

(6) Registrars should require accurate contact information from their clients, such as full name, address of domicile, telephone number and electronic mail, as well as information concerning a natural or legal person responsible for the technical operation of the domain name.

(7) The Registry policy should promote the use of all the official languages of the Community.

(8) Pursuant to Regulation (EC) No 733/2002, Member States may request that their official name and the name under which they are commonly known should not be registered directly under .eu TLD otherwise than by their national government. Countries that are expected to join the European Union later than May 2004 should be enabled to block their official names and the names under which they are commonly known, so that they can be registered at a later date.

(9) A Member State should be authorised to designate an operator that will register as a domain name its official name and the
name under which it is commonly known. Similarly, the Commission should be authorised to select domain names for use by the institutions of the Community, and to designate the operator of those domain names. The Registry should be empowered to reserve a number of specified domain names for its operational functions.

In accordance with Article 5(2) of Regulation (EC) No 733/2002, a number of Member States have notified to the Commission and to other Member States a limited list of broadly-recognised names with regard to geographical and/or geopolitical concepts which affect their political or territorial organisation. Such lists include names that could either not be registered or which could be registered only under the second level domain in accordance with the public policy rules. The names included in these lists are not subject to the first-come first-served principle.

The principle of first-come-first-served should be the basic principle for resolving a dispute between holders of prior rights during the phased registration. After the termination of the phased registration the principle of first come first served should apply in the allocation of domain names.

In order to safeguard prior rights recognised by Community or national law, a procedure for phased registration should be put in place. Phased registration should take place in two phases, with the aim of ensuring that holders of prior rights have appropriate opportunities to register the names on which they hold prior rights. The Registry should ensure that validation of the rights is performed by appointed validation agents. On the basis of evidence provided by the applicants, validation agents should assess the right which is claimed for a particular name. Allocation of that name should then take place on a first-come, first-served basis if there are two or more applicants for a domain name, each having a prior right.

The Registry should enter into an appropriate escrow agreement to ensure continuity of service, and in particular to ensure that in the event of re-delegation or other unforeseen circumstances it is possible to continue to provide services to the local Internet community with minimum disruption. The Registry should also comply with the relevant data protection rules, principles, guidelines and best practices, notably concerning the amount and type of data displayed in the WHOIS database. Domain names considered by a Member State court to be defamatory, racist or contrary to public policy should be blocked and eventually revoked once the court decision becomes final. Such domain names should be blocked from future registrations.

In the event of the death or insolvency of a domain name holder, if no transfer has been initiated at the expiry of the registration period, the domain name should be suspended for 40 calendar days. If the heirs or administrators concerned have not registered the name during that period it should become available for general registration.

Domain names should be open to revocation by the Registry on a limited number of specified grounds, after giving the domain name holder concerned an opportunity to take appropriate measures. Domain names should also be capable of revocation through an alternative dispute resolution (ADR) procedure.

The Registry should provide for an ADR procedure which takes into account the international best practices in this area and in particular the relevant World Intellectual Property Organization (WIPO) recommendations, to ensure that speculative and abusive registrations are avoided as far as possible.

The Registry should select service providers that have appropriate expertise on the basis of objective, transparent and non-discriminatory criteria. ADR should respect a minimum of uniform procedural rules, similar to the ones set out in the Uniform Dispute Resolution Policy adopted by the Internet Corporation of Assigned Names and Numbers (ICANN).

In view of the impending enlargement of the Union it is imperative that the system of public policy rules set up by this Regulation enter into force without delay.

The measures provided for in this Regulation are in accordance with the opinion of the Communications Committee established by Article 22(1) of Directive 2002/21/EC of the European Parliament and of the Council.

HAS ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER

Article 1

Subject matter

This Regulation sets out the public policy rules concerning the implementation and functions of the .eu Top Level Domain (TLD) and the public policy principles on registration referred to in Article 5(1) of Regulation (EC) No 733/2002.

CHAPTER II

PRINCIPLES ON REGISTRATION

Article 2

Eligibility and general principles for registration

An eligible party, as listed in Article 4(2)(b) of Regulation (EC) No 733/2002, may register one or more domain names under the .eu TLD. Without prejudice to Chapter IV, a specific domain name shall be allocated for use to the eligible party whose request has been received first by the Registry in the technically correct manner and in accordance with this Regulation. For the purposes of this Regulation, this criterion of first receipt shall be referred to as the “first-come-first-served” principle.

Once a domain name is registered it shall become unavailable for further registration until the registration expires without renewal, or until the domain name is revoked.

Unless otherwise specified in this Regulation, domain names shall be registered directly under the .eu TLD. Domain names registered under the .eu TLD shall only be transferable to parties that are eligible for registration of .eu domain names.

Article 3

Requests for domain name registration
The request for domain name registration shall include all of the following:
(a) the name and address of the requesting party;
(b) a confirmation by electronic means from the requesting party that it satisfies the general eligibility criteria set out in Article 4(2)(b) of Regulation (EC) No 733/2002;
(c) an affirmation by electronic means from the requesting party that to its knowledge the request for domain name registration is made in good faith and does not infringe any rights of a third party;
(d) an undertaking by electronic means from the requesting party that it shall abide by all the terms and conditions for registration, including the policy on the extra-judicial settlement of conflicts set out in Chapter VI.
Any material inaccuracy in the elements set out in points (a) to (d) shall constitute a breach of the terms of registration.
Any verification by the Registry of the validity of registration applications shall take place subsequently to the registration at the initiative of the Registry or pursuant to a dispute for the registration of the domain name in question, except for applications filed in the course of the phased registration procedure under Articles 10, 12, and 14.

Article 4

Accreditation of registrars

Only registrars accredited by the Registry shall be permitted to offer registration services for names under the .eu TLD. The procedure for the accreditation of registrars shall be determined by the Registry and shall be reasonable, transparent and non-discriminatory, and shall ensure effective and fair conditions of competition.
Registrars are required to access and use the Registry’s automated registration systems. The Registry may set further basic technical requirements for the accreditation of registrars.
The Registry may ask registrars for advance payment of registration fees, to be set annually by the Registry based on a reasonable market estimate.
The procedure, terms of accreditation of registrars and the list of accredited registrars shall be made publicly available by the Registry in readily accessible form.
Each registrar shall be bound by contract with the Registry to observe the terms of accreditation and in particular to comply with the public policy principles set out in this Regulation.

Article 5

Provisions for registrars

Without prejudice to any rule governing jurisdiction and applicable law, agreements between the Registrar and the registrant of a domain name cannot designate, as applicable law, a law other than the law of one of the Member States, nor can they designate a dispute-resolution body, unless selected by the Registrar pursuant to Article 23, nor an arbitration court or a court located outside the Community.
A registrar who receives more than one registration request for the same name shall forward those requests to the Registry in the chronological order in which they were received.
Only applications received after the date of accreditation shall be forwarded to the Registry.
Registrars shall require all applicants to submit accurate and reliable contact details of at least one natural or legal person responsible for the technical operation of the domain name that is requested.
Registrars may develop label, authentication and trustmark schemes in order to promote consumer confidence in the reliability of information that is available under a domain name that is registered by them, in accordance with applicable national and Community law.

CHAPTER III

LANGUAGES AND GEOGRAPHICAL CONCEPTS

Article 6

Languages

M3.1. Registrations of .eu domain names shall start only after the Registry has informed the Commission that the filing of applications for the registration of .eu domain names and communications of decisions concerning registration is possible in all official languages of the Community, hereinafter referred to as ‘official languages’.

M3.2. For any communication by the Registry that affects the rights of a party in conjunction with a registration, such as the grant, transfer, cancellation or revocation of a domain, the Registry shall ensure that these communications are possible in all official languages.

M3.3. The Registry shall perform the registration of domain names in all the alphabetic characters of the official languages when adequate international standards become available.

M3.4. If it becomes technically possible to register names in the official languages under the .eu TLD using alphabetic characters which were not available for registration at the beginning of the phased registration period provided for in Chapter IV, the Registry shall announce on its website that it will be possible to register names under the .eu TLD containing those characters.
The announcement shall contain a list of the characters in question and set out the date from which it will be possible to register .eu domain names using them.
The announcement shall be made three months before that date at the latest.

5. The Registry shall not be required to perform functions using languages other than the official languages.

Article 7

Procedure for reserved geographical and geopolitical names

For the procedure of raising objections to the lists of broadly recognised names in accordance with the third subparagraph of Article 5(2) of Regulation (EC) No 733/2002, objections shall be notified to the members of the Communications Committee established by Article 22(1) of Directive 2002/21/EC and to the Director-General of the Commission’s Directorate-General Information Society. The members of the Communications Committee and the Director-General may designate other contact points for these notifications.

Objections and designations of contact points shall be notified in the form of electronic mail, delivery by courier or in person, or by postal delivery effected by way of registered letter and acknowledgement of receipt.
Upon the resolution of any objections, the Registry shall publish on its website two lists of names. The one list shall contain the list of names that the Commission shall have notified to the Registry as ‘registrable only under a second level domain’.

M1. The list of names set out in the Annex to this Regulation shall only be reserved or registered as second level domain names directly under the .eu TLD by the countries indicated in the list.

Article 8

Reservation of names by countries and alpha-2 codes representing countries

1. The list of names set out in the Annex to this Regulation shall only be reserved or registered as second level domain names directly under the .eu TLD by the countries indicated in the list.

2. Alpha-2 codes representing countries shall not be registered as second level domain names directly under the .eu TLD.
Second level domain name for geographical and geopolitical names

►M3 1. ◄ Registration of geographical and geopolitical concepts as domain names in accordance with Article 5(2)(b) of Regulation (EC) No 733/2002 may be provided for by a Member State that has notified the names. This may be done under any domain name that has been registered by that Member State.

►M3 2. ◄ The Commission may ask the Registry to introduce domain names directly under the .eu TLD for use by the Community institutions and bodies. After the entry into force of this Regulation and not later than a week before the beginning of the phased registration period provided for in Chapter IV, the Commission shall notify the Registry of the names that are to be reserved and the bodies that represent the Community institutions and bodies in registering the names.

▼M3 3. If it becomes technically possible to register names in the official languages under the .eu TLD using alphabetic characters which were not available for registration at the beginning of the phased registration period provided for in Chapter IV, the Registry shall notify the Commission thereof.

That notification shall be made at the latest one month prior to the day of the announcement referred to in Article 6(4) and shall indicate the date of the announcement.

At the latest 10 working days before the date indicated in the announcement made in accordance with Article 6(4), the Commission shall ask the Registry to introduce any domain names containing one or more of those characters which it wishes to reserve for use by the Community institutions and bodies, directly under the .eu TLD.

CHAPTER IV
PHASED REGISTRATION

Article 10

Eligible parties and the names they can register

1. Holders of prior rights recognised or established by national and/or Community law and public bodies shall be eligible to apply to register domain names during a period of phased registration before general registration of .eu domain starts. 'Prior rights' shall be understood to include, inter alia, registered national and community trademarks, geographical indications, designations of origin, and, in so far as they are protected under national law in the Member-State where they are held: unregistered trademarks, trade names, business identifiers, company names, family names, and distinctive titles of protected literary and artistic works. 'Public bodies' shall include: institutions and bodies of the Community, national and local governments, governmental bodies, authorities, organisations and bodies governed by public law, and international and intergovernmental organisations.

2. The registration on the basis of a prior right shall consist of the registration of the complete name for which the prior right exists, as written in the documentation which proves that such a right exists.

3. The registration by a public body may consist of the complete name of the public body or the acronym that is generally used. Public bodies that are responsible for governing a particular geographic territory may also register the complete name of the territory for which they are responsible, and the name under which the territory is commonly known.

Article 11

Special characters

As far as the registration of complete names is concerned, where such names comprise a space between the textual or word elements, identity shall be deemed to exist between such complete names and the same names written with a hyphen between the word elements or combined in one word in the domain name applied for.

Where the name for which prior rights are claimed contains special characters, spaces, or punctuations, these shall be eliminated entirely from the corresponding domain name, replaced with hyphens, or, if possible, rewritten. Special character and punctuations as referred to in the second paragraph shall include the following:

- @ # $ % ^ & * ( ) + = <> { } \[ \]

Without prejudice to ►M3 Article 6(3) ◄, if the prior right name contains letters which have additional elements that cannot be reproduced in ASCII code, such as å, é or ô, the letters concerned shall be reproduced without these elements (such as a, e, n), or shall be replaced by conventionally accepted spellings (such as ae). In all other respects, the domain name shall be identical to the textual or word elements of the prior right name.

Article 12

Principles for phased registration

1. ►M1 Phased registration shall not start before the requirement of ►M3 Article 6(1)  ◄ is fulfilled. ◄

The Registry shall publish the date on which phased registration shall start at least two months in advance and shall inform all accredited Registrars accordingly.

The Registry shall publish on its website two months before the beginning of the phased registration a detailed description of all the technical and administrative measures that it shall use to ensure a proper, fair and technically sound administration of the phased registration period.

2. The duration of the phased registration period shall be four months. General registration of domain names shall not start prior to the completion of the phased registration period. Phased registration shall be comprised of two parts of two months each.

During the first part of phased registration, only registered national and Community trademarks, geographical indications, and the names and acronyms referred to in Article 10(3), may be applied for as domain names by holders or licensees of prior rights and by the public bodies mentioned in Article 10(1).

During the second part of phased registration, the names that can be registered in the first part as well as names based on all other prior rights can be applied for as domain names by holders of prior rights on those names.

3. The request to register a domain name based on a prior right under Article 10(1) and (2) shall include a reference to the legal basis in national or Community law for the right to the name, as well as other relevant information, such as trademark registration number, information concerning publication in an official journal or government gazette, registration information at professional or business associations and chambers of commerce.

4. The Registry may make the requests for domain name registration subject to payment of additional fees, provided that these serve merely to cover the costs generated by the application of this Chapter. The Registry may charge differential fees depending upon the complexity of the process required to validate prior rights.

5. At the end of the phased registration an independent audit shall be performed at the expense of the Registry and shall report its findings to the Commission. The auditor shall be appointed by the Registry after consulting the Commission. The purpose of the audit shall be to confirm the fair, appropriate and sound operational and technical administration of the phased registration period by the Registry.
6. To resolve a dispute over a domain name, the rules provided in Chapter VI shall apply.

**Article 13**

**Selection of validation agents**

Validation agents shall be legal persons established within the territory of the Community. Validation agents shall be reputable bodies with appropriate expertise. The Registry shall select the validation agents in an objective, transparent and non-discriminatory manner, ensuring the widest possible geographical diversity. The Registry shall require the validation agent to execute the validation in an objective, transparent and non-discriminatory manner.

Member States shall provide for validation concerning the names mentioned in Article 10(3). To that end, the Member States shall send to the Commission within two months following entry into force of this Regulation, a clear indication of the addresses to which documentary evidence is to be sent for verification. The Commission shall notify the Registry of these addresses.

The Registry shall publish information about the validation agents at its website.

**Article 14**

**Validation and registration of applications received during phased registration**

All claims for prior rights under Article 10(1) and (2) must be verifiable by documentary evidence which demonstrates the right under the law by virtue of which it exists.

The Registry, upon receipt of the application, shall block the domain name in question until validation has taken place or until the deadline passes for receipt of documentation. If the Registry receives more than one claim for the same domain during the phased registration period, applications shall be dealt with in strict chronological order.

The Registry shall make available a database containing information about the domain names applied for under the procedure for phased registration, and for each applicant, the Registrar that submitted the application, the deadline for submission of validation documents, and subsequent claims on the names.

Every applicant shall submit documentary evidence that shows that he or she is the holder of the prior right claimed on the name in question. The documentary evidence shall be submitted to a validation agent indicated by the Registry.

The applicant shall submit the evidence in such a way that it shall be received by the validation agent within forty days from the submission of the application for the domain name. If the documentary evidence has not been received by this deadline, the application for the domain name shall be rejected.

Validation agents shall time-stamp documentary evidence upon receipt.

Validation agents shall examine applications for any particular domain name in the order in which the application was received at the Registry.

The relevant validation agent shall examine whether the applicant that is first in line to be assessed for a domain name and that has submitted the documentary evidence before the deadline has prior rights on the name. If the documentary evidence has not been received in time or if the validation agent finds that the documentary evidence does not substantiate a prior right, he shall notify the Registry of this.

If the validation agent finds that prior rights exist regarding the application for a particular domain name that is first in line, he shall notify the Registry accordingly.

This examination of each claim in chronological order of rights shall be followed until a claim is found for which prior rights on the name in question are confirmed by a validation agent.

The Registry shall register the domain name, on the first come first served basis, if it finds that the applicant has demonstrated a prior right in accordance with the procedure set out in the second, third and fourth paragraphs.

**CHAPTER V**

**RESERVATIONS, WHOIS DATA AND IMPROPER REGISTRATIONS**

**Article 15**

**Escrow agreement**

1. The Registry shall, at its own expense, enter into an agreement with a reputable trustee or other escrow agent established within the territory of the Community designating the Commission as the beneficiary of the escrow agreement.

The Commission shall give its consent to that agreement before it is concluded. The Registry shall submit to the escrow agent a daily basis an electronic copy of the current content of the .eu database.

2. The agreement shall provide that the data shall be held by the escrow agent on the following terms and conditions:

(a) the data shall be received and held in escrow, undergoing no procedure other than verification that it is complete, consistent, and in proper format, until it is released to the Commission;

(b) the data shall be released from escrow upon expiration without renewal or upon termination of the contract between the Registry and the Commission for any of the reasons described therein and irrespectively of any disputes or litigation between the Commission and the Registry;

(c) in the event that the escrow is released, the Commission shall have the exclusive, irrevocable, royalty-free right to exercise or to have exercised all rights necessary to re-designate the Registry;

(d) if the contract with the Registry is terminated the Commission, with the cooperation of the Registry, shall take all necessary steps to transfer the administrative and operational responsibility for the .eu TLD and any reserve funds to such party as the Commission may designate: in that event, the Registry shall make all efforts to avoid disruption of the service and shall in particular continue to update the information that is subject to the escrow until the time of completion of the transfer.

**Article 16**

**WHOIS database**

The purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the domain names under the .eu TLD.

The WHOIS database shall contain information about the holder of a domain name that is relevant and not excessive in relation to the purpose of the database. In the event of the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder. The deliberate submission of inaccurate information, shall constitute grounds for considering the domain name registration to have been in breach of the terms of registration.

**Article 17**

**Names reserved by the Registry**

The following names shall be reserved for the operational functions of the Registry:
eurid.eu, registry.eu, niceu, dns.eu, internic.eu, whois.eu, das.eu, coc.eu, eurethix.eu, eurethics.eu, euthics.eu

**Article 18**
Improper registrations

Where a domain name is considered by a Court of a Member State to be defamatory, racist or contrary to public policy, it shall be blocked by the Registry upon notification of a Court decision and shall be revoked upon notification of a final Court decision. The Registry shall block from future registration those names which have been subject to such a court order for as long as such order remains valid.

Article 19

Death and winding up

1. If the domain name holder dies during the registration period of the domain name, the executors of his or her estate, or his or her legal heirs, may request transfer of the name to the heirs along with submission of the appropriate documentation. If, on expiry of the registration period, no transfer has been initiated, the domain name shall be suspended for a period of 40 calendar days and shall be published on the Registry's website. During this period the executors or the legal heirs may apply to register the name along with submission of the appropriate documentation. If the heirs have not registered the name during that 40-day period, the domain name shall thereafter become available for general registration.

2. If the domain name holder is an undertaking, a legal or natural person, or an organisation that becomes subject to insolvency proceedings, winding up, cessation of trading, winding up by court order or any similar proceeding provided for by national law, during the registration period of the domain name, then the legally appointed administrator of the domain name holder may request transfer to the purchaser of the domain name holders assets along with submission of the appropriate documentation. If, on expiry of the registration period, no transfer has been initiated, the domain name shall be suspended for a period of forty calendar days and shall be published on the registry's website. During this period the administrator may apply to register the name along with submission of the appropriate documentation. If the administrator has not registered the name during that 40-day period, the domain name shall thereafter become available for general registration.

CHAPTER VI

REVOCA TION AND SETTLEMENT OF CONFLICTS

Article 20

Revolocation of domain names

The Registry may revoke a domain name at its own initiative and without submitting the dispute to any extrajudicial settlement of conflicts, exclusively on the following grounds:

(a) outstanding unpaid debts owed to the Registry;
(b) holder's non-fulfilment of the general eligibility criteria pursuant to Article 4(2)(b) of Regulation (EC) 733/2002;
(c) holder's breach of the terms of registration under Article 3.

The Registry shall lay down a procedure in accordance with which it may revoke domain names on these grounds. This procedure shall include a notice to the domain name holder and shall afford him an opportunity to take appropriate measures.

Revocation of a domain name, and where necessary its subsequent transfer, may also be effected in accordance with a decision issued by an extrajudicial settlement body.

Article 21

Speculative and abusive registrations

1. A registered domain name shall be subject to revocation, using an appropriate extra-judicial or judicial, where that name is identical or confusingly similar to a name in respect of which a right is recognised or established by national and/or Community law, such as the rights mentioned in Article 10(1), and where it:

(a) has been registered by its holder without rights or legitimate interest in the name or;
(b) has been registered or is being used in bad faith.

2. A legitimate interest within the meaning of point (a) of paragraph 1 may be demonstrated where:

(a) prior to any notice of an alternative dispute resolution (ADR) procedure, the holder of a domain name or a name corresponding to the domain name in connection with the offering of goods or services or has made demonstrable preparation to do so;
(b) the holder of a domain name, being an undertaking, organisation or natural person, has been commonly known by the domain name, even in the absence of a right recognised or established by national and/or Community law;
(c) the holder of a domain name is making a legitimate and non-commercial or fair use of the domain name, without intent to mislead consumers or harm the reputation of a name on which a right is recognised or established by national and/or Community law.

3. Bad faith, within the meaning of point (b) of paragraph 1 may be demonstrated, where:

(a) circumstances indicate that the domain name was registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name to the holder of a name in respect of which a right is recognised or established by national and/or Community law or to a public body;
(b) the domain name has been registered in order to prevent the holder of such a name in respect of which a right is recognised or established by national and/or Community law, or a public body, from reflecting this name in a corresponding domain name, provided that:

(i) a pattern of such conduct by the registrant can be demonstrated;
(ii) the domain name has not been used in a relevant way for at least two years from the date of registration;
(iii) in circumstances where, at the time the ADR procedure was initiated, the holder of a domain name in respect of which a right is recognised or established by national and/or Community law or the holder of a domain name of a public body has declared his/her intention to use the domain name in a relevant way but fails to do so within six months of the day on which the ADR procedure was initiated;
(c) the domain name was registered primarily for the purpose of disrupting the professional activities of a competitor; or
(d) the domain name was intentionally used to attract Internet users, for commercial gain, to the holder of a domain name website or other on-line location, by creating a likelihood of confusion with a name on which a right is recognised or established by national and/or Community law or to a public body, such likelihood arising as to the source, sponsorship, affiliation or endorsement of the website or location or of a product or service on the website or location of the holder of a domain name; or
(e) the domain name registered is a personal name for which no demonstrable link exists between the domain name holder and the domain name registered.

4. The provisions in paragraphs 1, 2 and 3 may not be invoked so as to obstruct claims under national law.

Article 22

Alternative dispute resolution (ADR) procedure

1. An ADR procedure may be initiated by any party where:

(a) the registration is speculative or abusive within the meaning of Article 21; or
(b) a decision taken by the Registry conflicts with this Regulation or with Regulation (EC) No 733/2002.
2. Participation in the ADR procedure shall be compulsory for the holder of a domain name and the Registry.
3. A fee for the ADR shall be paid by the complainant.
4. Unless otherwise agreed by the parties, or specified otherwise in the registration agreement between registrar and domain name holder, the language of the administrative proceeding shall be the language of that agreement. This rule shall be subject to the authority of the panel to determine otherwise, having regard to the circumstances of the case.
5. The complaints and the responses to those complaints must be submitted to an ADR provider chosen by the complainant from the list referred to in the first paragraph of Article 23. That submission shall be made in accordance with this Regulation and the published supplementary procedures of the ADR provider.
6. As soon as a request for ADR is properly filed with the ADR provider and the appropriate fee is paid, the ADR provider shall inform the Registry of the identity of the complainant and the domain name involved. The Registry shall suspend the domain name involved from cancellation or transfer until the dispute resolution proceedings or subsequent legal proceedings are complete and the decision has been notified to the Registry.
7. The ADR provider shall examine the complaint for compliance with its rules of procedure, with the provisions of this Regulation and with Regulation (EC) No 733/2002, and, unless non-compliance is established, shall forward the complaint to the respondent within five working days following receipt of the fees to be paid by the complainant.
8. Within 30 working days of the date of receipt of the complaint the respondent shall submit a response to the provider.
9. Any written communication to a complainant or respondent shall be made by the preferred means stated by the complainant or respondent, respectively, or in the absence of such specification electronically via the Internet, provided that a record of transmission is available.
10. Failure of any of the parties involved in an ADR procedure to respond within the given deadlines or appear to a panel hearing may be considered as grounds to accept the claims of the counterparty.
11. In the case of a procedure against a domain name holder, the ADR panel shall decide that the domain name shall be revoked, if it finds that the registration is speculative or abusive as defined in Article 21. The domain name shall be transferred to the complainant if the complainant applies for this domain name and satisfies the general eligibility criteria set out in Article 4(2)(b) of Regulation (EC) No 733/2002.

The decision of the ADR panel shall state the date for implementation of the decision.

Decisions of the panel are taken by simple majority. The alternative dispute panel shall issue its decision within one month from the date of receipt of the response by the ADR provider. The decision shall be duly motivated. The decisions of the panel shall be published.

12. Within three working days after receiving the decision from the panel, the provider shall notify the full text of the decision to each party, the concerned registrar(s) and the Registry. The decision shall be notified to the Registry and the complainant by registered post or other equivalent electronic means.

13. The results of ADR shall be binding on the parties and the Registry unless court proceedings are initiated within 30 calendar days of the notification of the result of the ADR procedure to the parties.

Article 23

Selection of providers and panelists for alternative dispute resolution

1. The Registry may select ADR providers, who shall be reputable bodies with appropriate expertise in an objective, transparent and non-discriminatory manner. A list of the ADR providers shall be published on the Registry’s website.

2. A dispute which is submitted to the ADR procedure shall be examined by arbitrators appointed to a panel of one or three members.

The panelists shall be selected in accordance to the internal procedures of the selected ADR providers. They shall have appropriate expertise and shall be selected in an objective, transparent and non-discriminatory manner. Each provider shall maintain a publicly available list of panelists and their qualifications.

A panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the provider any circumstances giving rise to justifiable doubt as to their impartiality or independance. If, at any stage during the administrative proceedings, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the panelist, that panelist shall promptly disclose such circumstances to the provider.

In such event, the provider shall appoint a substitute panelist.

CHAPTER VII

FINAL PROVISIONS

Article 24

Entry into force

This Regulation shall enter into force on the day of its publication in the Official Journal of the European Union. This Regulation shall be binding in its entirety and directly applicable in all Member States. ▼M3
§ 1125. False designations of origin, false descriptions, and dilution forbidden

(a) Civil action
(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.
(2) As used in this subsection, the term “any person” includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity.

(b) Importation
Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States or admitted to entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this chapter in cases involving goods refused entry or seized.

(c) Dilution by blurring; dilution by tarnishment
(1) Injunctive relief
Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

(2) Definitions
(A) For purposes of paragraph (1), a mark is famous if it is widely recognized by the general consuming public of the United States as a designation of source of the goods or services of the mark's owner. In determining whether a mark possesses the requisite degree of recognition, the court may consider all relevant factors, including the following:
(i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.
(ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.
(iii) The extent of actual recognition of the mark.
(iv) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.
(B) For purposes of paragraph (1), “dilution by blurring” is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. In determining whether a mark or trade name is likely to cause dilution by blurring, the court may consider all relevant factors, including the following:
(i) The degree of similarity between the mark or trade name and the famous mark.
(ii) The degree of inherent or acquired distinctiveness of the famous mark.
(iii) The extent to which the owner of the famous mark is engaging in substantially exclusive use of the mark.
(iv) The degree of recognition of the famous mark.
(v) Whether the user of the mark or trade name intended to create an association with the famous mark.
(vi) Any actual association between the mark or trade name and the famous mark.
(C) For purposes of paragraph (1), “dilution by tarnishment” is association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.

(3) Exclusions
The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:
(A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
(i) advertising or promotion that permits consumers to compare goods or services; or
(ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
(B) All forms of news reporting and news commentary.
(C) Any noncommercial use of a mark.

(4) Burden of proof
In a civil action for trade dress dilution under this chapter for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that the matter sought to be protected is not functional.

Relevant “Anti-cybersquatting” provisions of the U.S. Code

TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1125

(a) Civil action
(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.
(2) As used in this subsection, the term “any person” includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity.

(b) Importation
Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States or admitted to entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this chapter in cases involving goods refused entry or seized.

(c) Dilution by blurring; dilution by tarnishment
(1) Injunctive relief
Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

(2) Definitions
(A) For purposes of paragraph (1), a mark is famous if it is widely recognized by the general consuming public of the United States as a designation of source of the goods or services of the mark's owner. In determining whether a mark possesses the requisite degree of recognition, the court may consider all relevant factors, including the following:
(i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.
(ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.
(iii) The extent of actual recognition of the mark.
(iv) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.
(B) For purposes of paragraph (1), “dilution by blurring” is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. In determining whether a mark or trade name is likely to cause dilution by blurring, the court may consider all relevant factors, including the following:
(i) The degree of similarity between the mark or trade name and the famous mark.
(ii) The degree of inherent or acquired distinctiveness of the famous mark.
(iii) The extent to which the owner of the famous mark is engaging in substantially exclusive use of the mark.
(iv) The degree of recognition of the famous mark.
(v) Whether the user of the mark or trade name intended to create an association with the famous mark.
(vi) Any actual association between the mark or trade name and the famous mark.
(C) For purposes of paragraph (1), “dilution by tarnishment” is association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.

(3) Exclusions
The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:
(A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
(i) advertising or promotion that permits consumers to compare goods or services; or
(ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
(B) All forms of news reporting and news commentary.
(C) Any noncommercial use of a mark.

(4) Burden of proof
In a civil action for trade dress dilution under this chapter for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that—
(A) the claimed trade dress, taken as a whole, is not functional and is famous; and
(B) if the claimed trade dress includes any mark or marks registered on the principal register, the unregistered matter,
taken as a whole, is famous separate and apart from any name of such registered marks.

(5) Additional remedies
In an action brought under this subsection, the owner of the famous mark shall be entitled to injunctive relief as set forth in section 1116 of this title. The owner of the famous mark shall also be entitled to the remedies set forth in sections 1117 (a) and 1118 of this title, subject to the discretion of the court and the principles of equity if—

(A) the mark or trade name that is likely to cause dilution by blurring or dilution by tarnishment was first used in commerce by the person against whom the injunction is sought after October 6, 2006; and

(B) in a claim arising under this subsection—

(i) by reason of dilution by blurring, the person against whom the injunction is sought willfully intended to trade on the recognition of the famous mark; or

(ii) by reason of dilution by tarnishment, the person against whom the injunction is sought willfully intended to harm the reputation of the famous mark.

(6) Ownership of valid registration a complete bar to action
The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register under this chapter shall be a complete bar to an action against that person, with respect to that mark, that—

(A) (i) is brought by another person under the common law or a statute of a State; and

(ii) seeks to prevent dilution by blurring or dilution by tarnishment; or

(B) asserts any claim of actual or likely damage or harm to the distinctiveness or reputation of a mark, label, or form of advertising.

(7) Savings clause
Nothing in this subsection shall be construed to impair, modify, or supersede the applicability of the patent laws of the United States.

(d) Cyberpiracy prevention

(1) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of title 36.

(B) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; or

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. 

(D) A person shall be liable for using a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(E) As used in this paragraph, the term "traffics in" refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.

(2) (A) The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if—

(i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c) of this section; and

(ii) the court finds that the owner—

(I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or

(II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by—

(aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and

(bb) publishing notice of the action as the court may direct promptly after filing the action.

(B) The actions under subparagraph (A)(ii) shall constitute service of process.

(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district in which—

(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(D)
(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—
(I) expeditiously deposit with the court documents sufficient to establish the court’s control and authority regarding the disposition of the registration and use of the domain name to the court; and
(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.

(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.

(cc) The Legal Information Institute - A Quick Overview http://www.law.cornell.edu/comments/credits.html
IV. Public Sector Information


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the European Economic and Social Committee (2),
Having regard to the opinion of the Committee of the Regions (3),
Acting in accordance with the procedure set out in Article 251 of the Treaty (4),

Whereas:

(1) The Treaty provides for the establishment of an internal market and of a system ensuring that competition in the internal market is not distorted. Harmonisation of the rules and practices in the Member States relating to the exploitation of public sector information contributes to the achievement of these objectives.

(2) The evolution towards an information and knowledge society influences the life of every citizen in the Community, inter alia, by enabling them to gain new ways of accessing and acquiring knowledge.

(3) Digital content plays an important role in this evolution. Content production has given rise to rapid job creation in recent years and continues to do so. Most of these jobs are created in small emerging companies.

(4) The public sector collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information.

(5) One of the principal aims of the establishment of an internal market is the creation of conditions conducive to the development of Community-wide services. Public sector information is an important primary material for digital content products and services and will become an even more important content resource with the development of wireless content services. Broad cross-border geographical coverage will also be essential in this context. Wider possibilities of re-using public sector information should inter alia allow European companies to exploit its potential and contribute to economic growth and job creation.

(6) There are considerable differences in the regulations and practices in the Member States relating to the exploitation of public sector information resources, which constitute barriers to bringing out the full economic potential of this key document resource. Traditional practice in public sector bodies in exploiting public sector information has developed in very disparate ways. That should be taken into account.

(7) Moreover, without minimum harmonisation at Community level, legislative activities at national level, which have already been initiated in a number of Member States in order to respond to the technological challenges, might result in even more significant differences. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased cross-border exploitation of information.

(8) A general framework for the conditions governing re-use of public sector documents is needed in order to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks. Use of such documents for other reasons constitutes a re-use. Member States’ policies can go beyond the minimum standards established in this Directive, thus allowing for more extensive re-use.

(9) This Directive does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use will remain with the Member States or the public sector body concerned. This Directive should apply to documents that are made accessible for re-use when public sector bodies license, sell, disseminate, exchange or give out information. To avoid cross-subsidies, re-use should include further use of documents within the organisation itself for activities falling outside the scope of its public tasks. Activities falling outside the public task will typically include supply of documents that are produced and charged for exclusively on a commercial basis and in competition with others in the market. The definition of ‘document’ is not intended to cover computer programmes. The Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents. It does not apply in cases in which citizens or companies can, under the relevant access regime, only obtain a document if they can prove a particular interest. At Community level, Articles 41 (right to good administration) and 42 of the Charter of Fundamental Rights of the European Union recognise the right of any citizen of the Union and any natural or legal person residing or having its registered office in a Member State to have access to European Parliament, Council and Commission documents. Public sector bodies should be encouraged to make available for re-use any documents held by them. Public sector bodies should promote and encourage re-use of documents, including official texts of a legislative and administrative nature in those cases where the public sector body has the right to authorise their re-use.

(10) The definitions of ‘public sector body’ and ‘body governed by public law’ are taken from the public procurement Directives (92/50/EEC (5), 93/36/EEC (6) and 93/37/EEC (7) and 98/43/EC (8)). Public undertakings are not covered by these definitions.

(11) This Directive lays down a generic definition of the term ‘document’, in line with developments in the information society. It covers any representation of acts, facts or
information — and any compilation of such acts, facts or information — whatever its medium (written on paper, or stored in electronic form or as a sound, visual or audiovisual recording), held by public sector bodies. A document held by a public sector body is a document where the public sector body has the right to authorize re-use.

(12) The time limit for replying to requests for re-use should be reasonable and in line with the equivalent time for requests to access the document under the relevant access regimes. Reasonable time limits throughout the Union will stimulate the creation of new aggregated information products and services at pan-European level. Once a request for re-use has been granted, public sector bodies should make the documents available in a timeframe that allows their full economic potential to be exploited. This is particularly important for dynamic content (eg, traffic data), the economic value of which depends on the immediate availability of the information and of regular updates. Should a licence be used, the timely availability of documents may be a part of the terms of the licence.

(13) The possibilities for re-use can be improved by limiting the need to digitise paper-based documents or to process digital files to make them mutually compatible. Therefore, public sector bodies should make documents available in any pre-existing format or language, through electronic means where possible and appropriate. Public sector bodies should view requests for extracts from existing documents favourably when creating such a request would involve only a simple operation. Public sector bodies should not, however, be obliged to provide an extract from a document where this involves disproportionate effort. To facilitate re-use, public sector bodies should make their own documents available in a format which, as far as possible and appropriate, is not dependent on the use of specific software. Where possible and appropriate, public sector bodies should take into account the possibilities for the re-use of documents by and for people with disabilities.

(14) Where charges are made, the total income should not exceed the total costs of collecting, producing, reproducing and disseminating documents, together with a reasonable return on investment, having due regard to the self-financing requirements of the public sector body concerned, where applicable. Production includes creation and collation, and dissemination may also include user support. Recovery of costs, together with a reasonable return on investment, consistent with applicable accounting principles and the relevant cost calculation method of the public sector body concerned, constitutes an upper limit to the charges, as any excessive prices should be precluded. The upper limit for charges set in this Directive is without prejudice to the right of Member States or public sector bodies, to apply lower charges or no charges at all, and Member States should encourage public sector bodies to make documents available at charges that do not exceed the marginal costs for reproducing and disseminating the documents.

(15) Ensuring that the conditions for re-use of public sector documents are clear and publicly available is a precondition for the development of a Community-wide information market. Therefore all applicable conditions for the re-use of the documents should be made clear to the potential re-users. Member States should encourage the creation of indices accessible in a timeframe where appropriate, of available documents so as to promote and facilitate requests for re-use. Applicants for re-use of documents should be informed of available means of redress relating to decisions or practices affecting them. This will be particularly important for SMEs which may not be familiar with interactions with public sector bodies from other Member States and corresponding means of redress.

(16) Making public all generally available documents held by the public sector — concerning not only the political process but also the legal and administrative process — is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. This objective is applicable to institutions at every level, be it local, national or international.

(17) In some cases the re-use of documents will take place without a licence being agreed. In other cases a licence will be issued imposing conditions on the re-use by the licensee dealing with issues such as liability, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be fair and transparent. Standard licences that are available online may also play an important role. In this respect, the Member States should provide for the availability of standard licences.

(18) If the competent authority decides to no longer make available certain documents for re-use, or to cease updating these documents, it should make these decisions publicly known, at the earliest opportunity, via electronic means whenever possible.

(19) Conditions for re-use should be non-discriminatory for comparable categories of re-use. This should, for example, not prevent the exchange of information between public sector bodies free of charge for the exercise of public tasks, whilst other parties are charged for the re-use of the same documents. Neither should it prevent the adoption of a differentiated charging policy for commercial and non-commercial re-use.

(20) Public sector bodies should respect competition rules when establishing the principles for re-use of documents avoiding as far as possible any exclusive agreements between themselves and private partners. However, in order to provide a service of general economic interest, an exclusive right to re-use specific public sector documents may sometimes be necessary. This may be the case if no commercial publisher would publish the information without such an exclusive right.

(21) This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data (9).

(22) The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term ‘intellectual property rights’ refers to copyright and related rights only (including sui generis forms of protection). This Directive does not apply to documents covered by industrial property rights, such as registered designs and trademarks. The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(23) Tools that help potential re-users to find documents available for re-use and the conditions for re-use can facilitate considerably the cross-border use of public sector documents. Member States should therefore ensure that practical arrangements are in place that help re-users in their search for documents available for re-use. Assets lists, accessible preferably online, of main documents (documents that are extensively re-used or that have the potential to be extensively re-used), and portal sites that are linked to decentralised assets lists are examples of such practical arrangements.

bodies can exercise their intellectual property rights in the
ternal information market when allowing re-use of
documents.
(25) Since the objectives of the proposed action, namely to
facilitate the creation of Community-wide information
products and services based on public sector documents, to
enhance an effective cross-border use of public sector
documents by private companies for added-value information
products and services and to limit distortions of competition
on the Community market, cannot be sufficiently achieved by
the Member States and can therefore, in view of the intrinsic
Community scope and impact of the said action, be better
achieved at Community level, the Community may adopt
measures, in accordance with the principle of subsidiarity as
set out in Article 5 of the Treaty. In accordance with the
principle of proportionality, as set out in that Article, this
Directive does not go beyond what is necessary in order to
achieve those objectives. This Directive should achieve
minimum harmonisation, thereby avoiding further disparities
between the Member States in dealing with the re-use of
public sector documents,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Directive establishes a minimum set of rules governing
the re-use and the practical means of facilitating re-use of
existing documents held by public sector bodies of the
Member States.

2. This Directive shall not apply to:

(a) documents the supply of which is an activity falling outside
the scope of the public task of the public sector bodies
considered as defined by law or by other binding rules in the
Member State, or in the absence of such rules, as defined in
line with common administrative practice in the Member State
in question, provided that the scope of the public tasks is
transparent and subject to review;

(b) documents for which third parties hold intellectual
property rights;

(c) documents which are excluded from access by virtue of the
access regimes in the Member States, including on the grounds
of:
— the protection of national security (i.e. State security),
defence, or public security,
— statistical confidentiality,
— commercial confidentiality (e.g. business, professional or
company secrets);

(ca) documents access to which is restricted by virtue of the
access regimes in the Member States, including cases whereby
citizens or companies have to prove a particular interest to
obtain access to documents;

(cb) parts of documents containing only logos, crests and
insignia;

(cc) documents access to which is excluded or restricted by
virtue of the access regimes on the grounds of protection of
personal data, and parts of documents accessible by virtue of
those regimes which contain personal data the re-use of which
has been defined by law as being incompatible with the law
concerning the protection of individuals with regard to the
processing of personal data;

(d) documents held by public service broadcasters and their
subsidiaries, and by other bodies or their subsidiaries for the
fulfilment of a public service broadcasting remit;

(e) documents held by educational and research
establishments, including organisations established for the
transfer of research results, schools and universities, except
university libraries and

(f) documents held by cultural establishments other than
libraries, museums and archives.

3. This Directive builds on and is without prejudice to access
regimes in the Member States.

4. This Directive leaves intact and in no way affects the level of
protection of individuals with regard to the processing of
personal data under the provisions of Union and national law,
and in particular does not alter the obligations and rights set
out in Directive 95/46/EC.

5. The obligations imposed by this Directive shall apply only
insofar as they are compatible with the provisions of
international agreements on the protection of intellectual
property rights, in particular the Berne Convention and the
TRIPS Agreement.

Article 2
Definitions

For the purpose of this Directive the following definitions shall
apply:

1. 'public sector body' means the State, regional or local
authorities, bodies governed by public law and associations
formed by one or several such authorities or one or several
such bodies governed by public law;

2. 'body governed by public law' means any body:

(a) established for the specific purpose of meeting needs in the
general interest, not having an industrial or commercial
character; and

(b) having legal personality; and

(c) financed, for the most part by the State, or regional or local
authorities, or other bodies governed by public law; or subject
to management supervision by those bodies; or having an
administrative, managerial or supervisory board, more than
half of whose members are appointed by the State, regional or
local authorities or by other bodies governed by public law;

3. 'document' means:

(a) any content whatever its medium (written on paper or
stored in electronic form or as a sound, visual or audiovisual
recording);

(b) any part of such content;

4. 're-use' means the use by persons or legal entities of
documents held by public sector bodies, for commercial or
non-commercial purposes other than the initial purpose
within the public task for which the documents were
produced. Exchange of documents between public sector
bodies purely in pursuit of their public tasks does not
constitute re-use;
5. ‘personal data’ means data as defined in Article 2(a) of Directive 95/46/EC.

6. ‘machine-readable format’ means a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure;

7. ‘open format’ means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

8. ‘formal open standard’ means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

9. ‘university’ means any public sector body that provides post-secondary-school higher education leading to academic degrees.

Article 3
General principle
1. Subject to paragraph 2 Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

2. For documents in which libraries, including university libraries, museums and archives hold intellectual property rights, Member States shall ensure that, where the re-use of such documents is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

CHAPTER II
REQUESTS FOR RE-USE

Article 4
Requirements applicable to the processing of requests for re-use

1. Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a timeframe of not more than 20 working days after its receipt. This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it.

2. Where no time limits or other rules regulating the timely provision of documents have been established, public sector bodies shall process the request and shall deliver the documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a timeframe of not more than 20 working days after its receipt. This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it.

3. In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or of the national provisions adopted pursuant to this Directive, in particular points (a) to (c) of Article 1(2) or Article 3. Where a negative decision is based on Article 1(2)(b), the public sector body shall include a reference to the natural or legal person who is the rightholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives shall not be required to include such a reference.

4. Any decision on re-use shall contain a reference to the means of redress in case the applicant wishes to appeal the decision. The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the national access to documents authority or a national judicial authority, whose decisions are binding upon the public sector body concerned.

5. Public sector bodies covered under Article 1(2)(d), (e) and (f) shall not be required to comply with the requirements of this Article.

CHAPTER III
CONDITIONS FOR RE-USE

Article 5
Available formats

1. Public sector bodies shall make their documents available in any pre-existing format or language, and, where possible and appropriate, in open and machine-readable format together with their metadata. Both the format and the metadata should, in so far as possible, comply with formal open standards.

2. Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

3. On the basis of this Directive, public sector bodies cannot be required to continue the production and storage of a certain type of documents with a view to the re-use of such documents by a private or public sector organisation.

Article 6
Principles governing charging

1. Where charges are made for the re-use of documents, those charges shall be limited to the marginal costs incurred for their reproduction, provision and dissemination.

2. Paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) by way of exception, documents for which the public sector body concerned is required to generate sufficient revenue to cover a substantial part of the costs relating to their collection, production, reproduction and dissemination. Those requirements shall be defined by law or by other binding rules in the Member State. In the absence of such rules, the requirements shall be defined in accordance with common administrative practice in the Member State;

(c) libraries, including university libraries, museums and archives.

3. In the cases referred to in points (a) and (b) of paragraph 2, the public sector bodies concerned shall calculate the total charges according to objective, transparent and verifiable criteria to be laid down by the Member States. The total income of those bodies from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction and
dissemination, together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved.

4. Where charges are made by the public sector bodies referred to in point (c) of paragraph 2, the total income from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved.

Article 7

Transparency

1. In the case of standard charges for the re-use of documents held by public sector bodies, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be pre-established and published, through electronic means where possible and appropriate.

2. In the case of charges for the re-use other than those referred to in paragraph 1, the public sector body in question shall indicate at the outset which factors are taken into account in the calculation of those charges. Upon request, the public sector body in question shall also indicate the way in which such charges have been calculated in relation to the specific re-use request.

3. The requirements referred to in point (b) of Article 6(2) shall be pre-established. They shall be published by electronic means, where possible and appropriate.

4. Public sector bodies shall ensure that applicants for re-use of documents are informed of available means of redress relating to decisions or practices affecting them.

Article 8

Licences

1. Public sector bodies may allow re-use without conditions or may impose conditions, where appropriate through a licence. These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage all public sector bodies to use the standard licences.

Article 9

Practical arrangements

Member States shall make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible Member States shall facilitate the cross-linguistic search for documents.

CHAPTER IV

NON-DISCRIMINATION AND FAIR TRADING

Article 10

Non-discrimination

1. Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use.

2. If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users.

Article 11

Prohibition of exclusive arrangements

1. The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights.

2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public.

This paragraph shall not apply to digitisation of cultural resources.

2a. Notwithstanding paragraph 1, where an exclusive right relates to digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. In case where that period exceeds 10 years, its duration shall be subject to review during the 11th year and, if applicable, every seven years thereafter.

The arrangements granting exclusive rights referred to in the first subparagraph shall be transparent and made public.

In the case of an exclusive right referred to in the first subparagraph, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

3. Exclusive arrangements existing on 1 July 2005 that do not qualify for the exceptions under paragraph 2 shall be terminated at the end of the contract or in any event not later than 31 December 2008.

4. Without prejudice to paragraph 3, exclusive arrangements existing on 17 July 2013 that do not qualify for the exceptions under paragraphs 2 and 2a shall be terminated at the end of the contract or in any event not later than 18 July 2043.

CHAPTER V

FINAL PROVISIONS

Article 12

Implementation

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 1 July 2005. They shall forthwith inform the Commission thereof.
When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 13

Review

1. The Commission shall carry out a review of the application of this Directive before 18 July 2018 and shall communicate the results of that review, together with any proposals for amendments to this Directive, to the European Parliament and the Council.

2. Member States shall submit a report every 3 years to the Commission on the availability of public sector information for re-use and the conditions under which it is made available and the redress practices. On the basis of that report, which shall be made public, Member States shall carry out a review of the implementation of Article 6, in particular as regards charging above marginal cost.

3. The review referred to in paragraph 1 shall in particular address the scope and impact of this Directive, including the extent of the increase in re-use of public sector documents, the effects of the principles applied to charging and the re-use of official texts of a legislative and administrative nature, the interaction between data protection rules and re-use possibilities, as well as further possibilities of improving the proper functioning of the internal market and the development of the European content industry.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Union.

---

**Relevant Case Law on Public Sector Information**

**Case C-343/95, Diego Calì & Figli Srl v Servizi Ecologici Porto di Genova SpA (SEPG)**

(...)

13 In the course of the proceedings contesting that order, the Tribunale di Genova stayed proceedings until the Court of Justice had given a preliminary ruling on the following questions:

1. Can a "dominant position within the common market or in a substantial part of it" be said to exist where a limited company, set up by a national port authority, is given administrative concession from that authority, the task of providing with exclusive rights within a harbour sector specializing in loading and unloading petroleum products, an "anti-pollution surveillance" service, and where that company collects the relevant fee, which is set unilaterally by the port authority on the basis of the vessel’s tonnage and the quantity of the product loaded or unloaded, from users of that service, that is, to say vessels which dock at the wharves to carry out those operations?

2. Having regard to the situation set out in Question 1 and if there is a dominant position within the common market or a substantial part of it, is there an abuse of the aforesaid "dominant position" within the meaning of Article 86 of the Treaty, in particular of subparagraphs (a), (c) and (d), and are there related practices, when an undertaking holding the exclusive concession for a service (even though on the basis of a decision of the authority granting the concession) charges fees:

- which are compulsory and independent of the provision of an efficient surveillance and/or intervention service, merely because a vessel berths in a mooring in the Porto Petroli and loads/unloads goods, whether petroleum products or chemicals and petrochemicals, according to the contractual terms imposed;
- the amount of which depends solely on the tonnage of the vessel, the amount of the product and also, in the event of any actual intervention, the duration thereof, but not on the product’s nature, quality or capacity to pollute;
- which, since they are imposed exclusively on the vessel (which is merely passively loaded and unloaded), affect a subject other than those whose responsibility it is to carry out the necessary technical operations (in this case Porto Petroli di Genova SpA and the laders/receivers of the product), resulting in an inevitable discrepancy between the responsibility for any pollution and the bearing of the cost of the anti-pollution service;
- which, given the nature of the product and/or its existence, represent an unnecessary service for vessels equipped with their own anti-pollution devices and systems adapted to the type of product to be loaded or unloaded;

---

109
which impose on the vessel a charge, and an associated extra cost, in addition to those provided for by the landing contract between the carrier and the company operating the wharves, and have no practical connection with the subject-matter of the contract.

3. If, in the situations set out in Questions 1 and 2, there are one or more practices amounting to abuse of a dominant position by an undertaking for the purposes of Article 86 of the Treaty, does this lead to a potential adverse effect on trade between Member States of the Union?

(…)

Findings of the Court

135. Under the rules which govern procedure in cases before the Court of First Instance, parties are entitled to protection against the misuse of pleadings and evidence. Thus, in accordance with the third subparagraph of Article 5(3) of the Rules of Procedure, the President may exclude secret or confidential documents from those furnished to an intervenor in a case.

136. These provisions reflect a general principle in the due administration of justice according to which parties have the right to defend their interests free from all external influences and particularly from influences on the part of members of the public.

137. It follows that a party who is granted access to the procedural documents of other parties is entitled to use those documents only for the purpose of pursuing his own case and for no other purpose, including that of inciting criticism on the part of the public in relation to arguments raised by other parties in the case.

138. In the present case, it is clear that the actions of the applicant in publishing an edited version of the defence on the Internet in conjunction with an invitation to the public to send their comments to the Agents of the Council and in providing the telephone and telefax numbers of those Agents, had as their purpose to bring pressure to bear upon the Council and to provoke public criticism of the Agents of the institution in the performance of their duties.

139. These actions on the part of the applicant involved an abuse of procedure which will be taken into account in awarding costs (see below, paragraph 140), having regard, in particular, to the fact that this incident led to a suspension of the proceedings and made it necessary for the parties in the case to lodge additional submissions in this respect.

(…)

On those grounds,

THE COURT OF FIRST INSTANCE (Fourth Chamber, Extended Composition)

hereby:

1. Annulls the Council’s decision of 6 July 1995 refusing the applicant access to certain documents relating to the European Police Office (Europol);
2. Orders the Council to pay two-thirds of the applicant’s costs as well as its own costs;
3. Orders the Kingdom of Denmark, the French Republic, the Kingdom of the Netherlands, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland to bear their own costs.


Case C-7/13, Creditinfo Lánstraust hf. and Registers Iceland and the Icelandic State

(…)

13 The plaintiff is engaged in recording and communicating information on financial matters and creditworthiness, and related services. In the course of its business, it seeks information and data from public sector bodies, including the first defendant, Registers Iceland.

14 Between 2004 and 2007, the plaintiff entered into a series of contracts with the National Land Registry concerning access to information. In 2010, the National Land Registry merged with the National Registry to form Registers Iceland.

15 Registers Iceland has charged the plaintiff fees for the disclosure of information and data. The plaintiff has brought an action before the national court for the repayment of fees for the period between 11 January 2008 and 31 December 2011. Since the tariffs were approved by the Minister of Finance, the plaintiff also brings its action against the Icelandic State.

16 In its request, registered at the Court on 29 April 2013, Reykjavík District Court has referred the following questions:

1. Is it compatible with EEA law, and specifically with Article 6 of Council Directive 2003/98/EC, on the re-use of public sector information (cf. The Decision of the EEA Joint Committee, No 105/2005, amending Annex XI (Telecommunication services) to the EEA Agreement), to charge a fee on account of each mechanical enquiry for information from the register if no calculation of the ‘total income’ and the ‘cost’, in the sense of Article 6 of the Directive, is available at the time of the determination of the fee?

2. Is it compatible with Article 6 of the Directive if, when the ‘cost’ subject to Article 6 of the Directive is determined, no account is taken of:
   a. income accruing to the State when documents are collected, in the form of fees paid by individuals and undertakings for the recording of contracts in the registers of legal deeds, and
   b. income accruing to the State when documents are collected, in the form of taxes which are levied as stamp duties on recorded legal deeds at the time when individuals and undertakings apply to have them recorded in the registers of legal deeds?

3. Is it compatible with Article 6 of the Directive if, when the ‘cost’ pursuant to Article 6 of the Directive is determined, account is taken of costs incurred by a public sector body in connection with the collection of documents which it is legally obliged to collect, irrespective of whether or not individuals or undertakings request to re-use them?

4. Is it compatible with Article 6 of the Directive if, when the ‘cost’ pursuant to the article is determined, the legislature sets the amount of the fee in legislation without any particular assessment of the ‘total income’ and the cost?

5. Would it be compatible with Article 6 of the Directive if, when the ‘cost’ pursuant to the Directive is determined, appropriate account was taken of a general requirement in national legislation that public sector bodies be self-financing?

6. If the answer to Question No 5 is in the affirmative, what does this involve in further detail and what cost elements in public sector operations may be taken into account in this context?

(…)

33 Recital 5 of the preamble to the Directive states that public sector data are an important primary material for digital content products and services. European companies should be able to exploit their potential and contribute to economic growth and job creation.

34 Public sector information is a key resource for industry in the information society (see the Commission’s Green Paper, COM(1998)585). A main goal of the European legislature was to put European firms on an equal footing with their American counterparts, which, since the enactment of the Freedom of Information Act in 1966, have benefited from a highly developed, efficient public information system at all levels of the administration. The Commission has highlighted that the US government’s active policy of ensuring both access to and commercial exploitation of public sector information has greatly stimulated the development of the US information industry (see the Commission’s Green Paper, cited above, p. 1).
35 According to its Article 1, the Directive establishes a minimum set of rules governing re-use and the practical means of facilitating the re-use of existing documents held by public sector bodies. In Article 2(4) of the Directive, re-use is defined as use for any commercial or non-commercial purpose other than the initial purpose for which the documents were produced.

36 It is clear from recital 9 of the preamble that, although the Directive does not contain any obligation to allow re-use, public sector bodies should be encouraged to make any documents held by them available for re-use.

37 Where re-use is authorised, and where charges are made for that purpose, it is an objective of the Directive, as set out in recital 14 of its preamble, to preclude excessive pricing. It must be borne in mind in this context that the public bodies in question are normally monopolies.

38 Article 6 of the Directive therefore states that charges may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment.

39 Pricing is a crucial issue in relation to the exploitation of public sector information by the digital content industries. It largely determines whether they will find an interest in investing in value added products and services based on public sector information. American companies benefit from the fact that they can obtain US public sector information free of charge (the Commission's Green Paper, cited above, p. 14). If European companies are to be put on an equal footing with their competitors in other parts of the world, the cost elements and return on investment cannot be calculated in a way that would put them at a significant disadvantage. It is for the national court to assess the facts in that respect, in particular with regard to the relevant interest level. It must therefore take into account that Article 6 of the Directive does not aim to provide public sector bodies with a profit.

40 Moreover, pursuant to Article 7 of the Directive, standard charges for the re-use of documents shall be pre-established and published. The public sector body shall indicate the calculation basis for the published charge if requested to do so. This should be done in order to enable individuals and economic operators charged for re-use of public information to verify whether the charges in question are compatible with Article 6 of the Directive. The Directive does not require that the calculation basis be made available at the time when the charge is fixed. Nevertheless, the requirement that standard charges within the limit set by Article 6 shall be pre-established presupposes that a substantive examination has been undertaken at the time when the charge is fixed. This must apply irrespective of whether the charge is set in legislation, by the relevant public authority or by other means.

41 As regards the calculation basis for the charges, national courts may have to apply the principle of effectiveness (compare Alakor, cited above, paragraph 26, and case law cited).

42 The first question must therefore be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

43 The second question must be that, where rationally possible, the standard charges are pre-established and published, and that, where rationally possible, the calculation basis is made available at the time when the charge is fixed.

44 An exception to the repayment obligation applies when repayment entails unjust enrichment. Repayment is not required if it is established that the person required to pay unlawful charges has actually passed them on to other persons (see, for comparison, Alakor, cited above, paragraph 25, and case law cited). Such an exception must however be interpreted restrictively (see, for comparison, most recently, Case C-398/09 Lady & Kid and Others [2011] ECR I-7575, paragraph 20).

45 It is for the domestic legal system of each EEA State to lay down the procedural rules governing such repayments. However, these rules must not be less favourable than those governing similar domestic actions (the principle of equivalence), and must not render practically impossible or excessively difficult the exercise of rights conferred by EEA law (the principle of effectiveness) (compare Alakor, cited above, paragraph 26, and case law cited).

46 Consequently, the question of whether a charge levied in violation of EEA law has or has not been passed on is a question of fact to be determined by the national court, taking all relevant circumstances into account.

47 Where a charge levied in violation of EEA law is passed on, depends on the circumstances of the case, in particular the market structure. For example, a monopoly operator can be expected to pass on the entire charge. If there is competition, an operator may not be able to pass on any part of it (compare with regard to this conclusion the judgment of the Supreme Court of Norway of 28 May 2008 in case 2007/1738, Rt. 2008 p. 738, paragraph 52). Moreover, even where it is established that the charge has been passed on in whole or in part to customers, repayment does not necessarily entail unjust enrichment. The charged person may still suffer a loss, in particular as a result of a fall in the volume of his sales (see, for comparison, Lady & Kid and Others, cited above, paragraph 21, and case law cited).

48 As regards the specific situation where a charge for the re-use of public information set out in legislation has proven to be excessive, the court recalls that the national courts must apply the methods of interpretation recognised by national law as far as possible in order to achieve the result sought by the relevant EEA law rule (see, inter alia, Case E-7/11 Grund [2012] EFTA Ct. Rep. 191, paragraph 83, and case law cited).

49 The answer to the first and fourth questions must therefore be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

50 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

51 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

52 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

53 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

54 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

55 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

56 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

57 The second question must be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantiative examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the rate of return for profit-seeking activities may not fall below the average return on investment.

58 As mentioned above, Article 6 of the Directive provides that, where charges are made, they may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment.

59 It follows from the wording that cost within the meaning of this provision is not limited to the cost of facilitating re-use, that is, reproduction and dissemination. Account may be taken of the cost incurred by a public sector body in connection with the initial collection and production of the documents in question. This must apply irrespective of whether the public sector body was legally obliged to collect the documents, as the Directive makes no such distinction.

60 Recital 14 of the preamble emphasises that States should encourage public sector bodies to make documents available at charges that do not exceed the marginal cost of reproducing and disseminating them. It should also be kept in mind that the Directive has recently been amended by...
Directive 2013/37/EU. Once the amendment has entered into force, the main rule under the new Article 6 will be that the cost of collection and production cannot be taken into account. 61 However, under the Directive, if account is taken of cost incurred by a public sector body in connection with the initial collection and production of documents, any income accrued in that respect, for example fees or taxes such as stamp duties, which reduce or offset that cost, must also be taken into account. Consequently, the cost within the meaning of Article 6 must be construed as the net cost. If only the cost incurred as a result of collection were to be taken into account and not the income accrued in that connection, this would undermine the effectiveness of the Directive's objective of precluding excessive pricing.

62 It is for the national court to examine the facts of the case before it in order to determine the cost that may, on the basis of the above, be taken into consideration pursuant to Article 6. 63 The answer to the second and third questions must therefore be that, when the cost pursuant to Article 6 of the Directive is determined, account may be taken of the cost incurred by a public sector body in connection with the initial collection and production of the documents in question. In such case, any income accrued in that connection, for example fees or taxes such as stamp duties, which reduce or offset that cost, must also be taken into account.

[---]

70 Article 6 of the Directive provides that charges may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment, having due regard to any self-financing requirements of the public sector body concerned, as stated in recital 14 of the preamble to the Directive. 71 Accordingly, general or specific self-financing requirements for public sector bodies may be taken into account when determining the cost pursuant to Article 6 of the Directive. Nonetheless, as argued by both ISA and the Commission, the cost within the meaning of Article 6, together with a reasonable return on investment, must relate to the handling of documents, either their initial collection or production, or the actual facilitation of re-use through reproduction and dissemination. Consequently, when charges are made, cost elements and investments that are unrelated to the document processing necessary for re-use set out in Article 6 may not be taken into account. These principles governing charging in Article 6 must be the same irrespective of any self-financing requirement to which the public body in question is subject. 72 At the oral hearing, the defendants implied, in response to a question put to them, that the charges for re-use in dispute in the case before the national court are also used to cover the cost of services that the plaintiff itself has not received from Registers Iceland. If it is established that the charges are used to cover cost other than that related to the collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment in the facilitation of re-use, those charges are contrary to Article 6. It is for the national court to make the assessment. 73 The answer to the fifth and sixth questions must therefore be that self-financing requirements for public sector bodies may be taken into account when determining the cost under Article 6 of the Directive. This applies insofar as only cost elements, together with a reasonable return on investment, that are related to the document processing necessary for re-use set out in Article 6 are taken into account.

[---]

10 TU Darmstadt operates a regional and academic library in which it installed electronic reading points that allow the public to consult works contained in the collection of that library. 11 Since January or February 2009, those works have included the textbook of Schulze W., Einführung in die neuere Geschichte ('the textbook at issue'), published by Ulmer, a scientific publishing house established in Stuttgart (Germany). 12 TU Darmstadt did not take up Ulmer's offer of 29 January 2009 of an opportunity to purchase and use the textbooks it publishes as electronic books ('e-books'), including the textbook at issue.

13 TU Darmstadt digitised that textbook so as to make it available to users on electronic reading points installed in its library. Those points did not allow for a greater number of copies of that work to be consulted at any one time than the number owned by the library. Users of the reading points could print out the work on paper or store it on a USB stick, in part or in full, and take it out of the library in that form. 14 In an action brought by Ulmer, the Landgericht (Regional Court) Frankfurt am Main held, by judgment of 6 March 2011, that the rightholder and establishment must have reached prior agreement on the digital use of the work concerned for Paragraph 52b of the UrhG not to apply. That court also rejected Ulmer's application seeking to prohibit TU Darmstadt from digitising the textbook at issue or having it digitised. However, it granted that company's request to prohibit users of the TU Darmstadt library from being able, at electronic reading points installed therein, to print out that work and/or store it on a USB stick and/or take such reproductions out of the library. 15 Hearing an appeal by Ulmer, the Bundesgerichtshof (Federal Court of Justice) considers, in the first place, that the question arises whether works and other protected objects are 'subject to purchase or licensing terms', within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder offers to conclude with an establishment referred to in that provision appropriately worded licensing agreements in respect of those works or whether a different interpretation of that provision must be adopted, in terms of which only cases where the owner and the establishment have entered into an agreement on that matter are covered. 16 That court takes the view that, unlike the German language version of the provision, the English and French language versions are consistent with the first of the above interpretations. That interpretation could also be justified on
the basis of the purpose and general scheme of Directive 2001/29. However, if only the entering into an agreement would allow for the application of that provision to be ruled out, it would be open to the establishment to refuse an appropriate offer from the rightholder so as to benefit from the limiting provision in question, which would also mean that the owner would not receive appropriate remuneration, which nevertheless is one of the objectives of that directive.

17 In the second place, the referring court is uncertain whether Article 5(3)(n) of Directive 2001/29 must be interpreted so as to mean that it allows Member States to confer on the establishments referred to in that provision the right to digitise the works contained in their collections to the extent that the communication or making available of those works on their terminals requires such reproduction. The referring court takes the view that Member States should have an ancillary competence in order to provide for such an exception to the reproduction right referred to in Article 2 of that directive or such a limitation of that right; otherwise the effectiveness of Article 5(3)(n) would not be guaranteed. That competence could, in any event, be inferred from Article 5(2)(c) of the directive.

18 In the third place, the referring court takes the view that the dispute in the main proceedings raises the question whether, pursuant to Article 5(3)(n) of Directive 2001/29, Member States may provide for a limiting provision permitting the users of an establishment referred to in that provision to print out on paper or store on a USB stick, in part or in full, the works reproduced or made available by the establishment on its terminals.

19 In that regard, that court considers, first of all, that while those printouts, stored copies or downloads, being related to the reproduction of a work, are not, in principle, covered by the limitations provided for in Article 5(3)(n) of Directive 2001/29, they could nevertheless be permitted, as an extension of the communication or of the making available of a work by the establishment in question, under another limitation, in particular, pursuant to the so-called ‘private copying’ exception provided for in Article 5(2)(b) of that directive.

20 Next, the court finds that the objective referred to in Article 5(3)(n) of Directive 2001/29, which entails permitting the efficient use, for the purpose of research or private study, of texts communicated or made available on the terminals of an establishment such as a library, is consistent with an interpretation of that provision to the effect that the printing out on paper of a work from a terminal should be permitted, whereas storage on a USB stick should not be.

21 Lastly, the referring court considers that such an interpretation of Article 5(3)(n) of Directive 2001/29 would also ensure that the scope of the limitation provided for in that provision respects the threefold condition provided for in Article 5(5) of that directive. In its view, storage of a work on a USB stick encroaches upon the rights of the author of that work more than printing it out on paper.

22 In those circumstances, the Bundesgerichtshof decided to stay the proceedings and refer the following questions to the Court for a preliminary ruling:

(1) Is a work subject to purchase or licensing terms, within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder has offered to conclude with the establishments referred to therein licensing agreements for the use of that work on appropriate terms?

(2) Does Article 5(3)(n) of Directive 2001/29 entitle the Member States to confer on those establishments the right to digitise the works contained in their collections, if that is necessary in order to make those works available on terminals?

(3) May the rights which the Member States lay down pursuant to Article 5(3)(n) of Directive 2001/29 go so far as to enable users of the terminals to print out on paper or store on a USB stick the works made available there?

23 By its first question, the referring court is essentially asking whether a work is subject to ‘purchase or licensing terms’, within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder has offered to conclude with an establishment referred to in that provision, such as a publicly accessible library, one appropriately worded terms a licensing agreement in respect of that work.

24 All of the interested parties that have presented written observations, with the exception of Ulmer, propose that the first question be answered in the negative and essentially support an interpretation to the effect that the concept of ‘purchase or licensing terms’, mentioned in Article 5(3)(n) of Directive 2001/29, must be understood to mean that the rightholder and establishment concerned must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use the work.

25 Ulmer argues that the mere fact that the rightholder offers to conclude a licensing agreement with a publicly accessible library is sufficient for ruling out the application of Article 5(3)(n) of Directive 2001/29, provided always that such offer is ‘appropriate’.

26 In that regard, first of all, a comparison of the language versions of Article 5(3)(n) of Directive 2001/29, particularly the English, French, German and Spanish versions — which use the words ‘terms’, ‘conditions’, ‘Regelung’ and ‘condiciones’, respectively — shows that, in that provision, the EU legislature used the concept ‘terms’ or ‘provisions’, which refer to contractual terms actually agreed as opposed to mere contractual offers.

27 Next, it should be recalled that the limitation under Article 5(3)(n) of Directive 2001/29 aims to promote the public interest in promoting research and private study, through the dissemination of knowledge, which constitutes, moreover, the core mission of publicly accessible libraries.

28 The interpretation favoured by Ulmer implies that the rightholder could, by means of a unilateral and essentially discretionary action, deny the establishment concerned the right to benefit from that limitation and thereby prevent it from realising its core mission and promoting the public interest.

29 Moreover, recital 40 in the preamble to Directive 2001/29 states that specific contracts or licences should be promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve.

30 As noted by the Advocate General in points 21 and 22 of his Opinion, recitals 45 and 51 in the preamble to Directive 2001/29 confirm (including in their German version) that, in the context, inter alia, of the exceptions and limitations listed in Article 5(3) of Directive 2001/29, it is existing contractual relations and the conclusion and implementation of existing contractual agreements that are at issue, and not mere prospects of contracts or licences.

31 Furthermore, the interpretation proposed by Ulmer is difficult to reconcile with the aim pursued by Article 5(3)(n) of Directive 2001/29, which is to maintain a fair balance between the rights and interests of rightholders, on the one hand, and, on the other hand, users of protected works who wish to communicate them to the public for the purpose of research or private study undertaken by individual members of the public.

32 In addition, if the mere act of offering to conclude a licensing agreement were sufficient to rule out the application of Article 5(3)(n) of Directive 2001/29, such an interpretation would be liable to negate much of the substance of the limitation provided for in that provision, or indeed its effectiveness, since, were it to be accepted, the limitation would apply, as Ulmer has maintained, only to those increasingly rare works of which an electronic version, primarily in the form of an e-book, is not yet offered on the market.

33 Lastly, the interpretation to the effect that there must be contractual terms actually agreed also cannot be ruled out — contrary to what is maintained by Ulmer — by reason of the
fact that it would conflict with the threefold condition provided for in Article 5(5) of Directive 2001/29.

34. In that regard, it is sufficient to state that the limitation provided for in Article 5(3)(n) of Directive 2001/29 is accompanied by a number of restrictions that guarantee — even though the application of that provision is ruled out only in the event that contractual terms have actually been concluded — the continuing applicability of such a limitation in special cases which do not conflict with a normal exploitation of the works and do not unreasonably prejudice the legitimate interests of the rightholder.

35. In the light of the foregoing considerations, the answer to the first question is that the concept of ‘purchase or licensing terms’ provided for in Article 5(3)(n) of Directive 2001/29 must be understood as requiring that the rightholder and an establishment, such as a publicly accessible library, referred to in that provision must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use that work.

The second question

36. By its second question, the referring court is essentially asking whether Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it precludes Member States from granting to publicly accessible libraries covered by that provision the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

37. The first point to be noted is that the digitisation of a work, which essentially involves the conversion of the work from an analogue format into a digital one, constitutes an act of reproduction of the work.

38. The question therefore arises whether Article 5(3)(n) of Directive 2001/29 permits Member States to grant that reproduction right to publicly accessible libraries, since, under Article 2 of that directive, it is the authors that have the exclusive right to authorise or prohibit the reproduction of their works.

39. In that regard, it should first be stated that, according to the first sentence of Article 5(3) of Directive 2001/29, the exceptions and limitations set out in that paragraph relate to the rights provided for in Articles 2 and 3 of that directive and thus both the exclusive reproduction right enjoyed by the rightholder and the right of communication to the public of works.

40. However, Article 5(3)(n) of the directive limits the use of works, within the meaning of that provision, to the ‘communication or making available’ of those works and thus to acts which fall under the sole exclusive right of communication to the public of works referred to in Article 3 of that directive.

41. Next, it should be recalled that for there to be an ‘act of communication’ for the purposes of Article 3(1) of Directive 2001/29, it is sufficient, in particular, that those works are made available to a public in such a way that the persons forming that public may access them, irrespective of whether they avail themselves of that opportunity (judgment in Svensson and Others, C‑466/12, EU:C:2014:76, paragraph 19).

42. It follows that, in circumstances such as those of the case in the main proceedings, where an establishment, such as a publicly accessible library, which falls within Article 5(3)(n) of Directive 2001/29, gives access to a work contained in its collection to a ‘public’, namely all of the individual members of the public using the dedicated terminals installed on its premises for the purpose of research or private study, that must be considered to be ‘making [that work] available’ and, therefore, an ‘act of communication’ for the purposes of Article 3(1) of that directive (see, to that effect, judgment in Svensson and Others, EU:C:2014:76, paragraph 20).

43. Such a right of communication of works enjoyed by establishments such as publicly accessible libraries covered by Article 5(3)(n) of Directive 2001/29, within the limits of the conditions provided for by that provision, would risk being rendered largely meaningless, or indeed ineffective, if those establishments did not have an ancillary right to digitise the works in question.

44. Those establishments are recognised as having such a right pursuant to Article 5(2)(c) of Directive 2001/29, provided that specific acts of reproduction are involved.

45. That condition of specificity must be understood as meaning that, as a general rule, the establishments in question may not digitise their entire collections.

46. However, that condition is, in principle, observed where the digitisation of some of the works of a collection is necessary for the purpose of the ‘use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals’, as provided in Article 5(3)(n) of Directive 2001/29.

47. Furthermore, the scope of that ancillary right of digitisation must be determined by interpreting Article 5(2)(c) of Directive 2001/29 in the light of Article 5(5) of that directive, under which that limitation is applicable only in certain special cases which do not prejudice the normal exploitation of the work or other protected object or cause unjustified harm to the legitimate interests of the rightholder, the latter provision, however, not being intended to extend the scope of the exceptions and limitations provided for in Article 5(2) of the directive (see, to that effect, judgments in Infopaq International, C‑5/08, EU:C:2009:465, paragraph 56, and ACI Adam and Others, C‑435/12, EU:C:2014:254, paragraph 26).

48. In the present case, it must be stated that the applicable national legislation takes due account of the conditions provided for in Article 5(5) of the directive, since it follows, first, from Article 52b of the UrhG, that the digitisation of works by publicly accessible libraries cannot have the result of the number of copies of each work made available to users by dedicated terminals being greater than that of those libraries have acquired in analogue format. Secondly, although, by virtue of that provision of national law, the digitisation of the work is not, as such, coupled with an obligation to provide compensation, the subsequent making available of that work in digital format, on dedicated terminals, gives rise to a duty to make payment of adequate remuneration.

49. Having regard to the foregoing considerations, the answer to the second question is that Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

The third question

50. By its third question, the referring court is essentially asking whether Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it precludes Member States from granting to publicly accessible libraries covered by that provision the right to make works available to users by dedicated terminals which permit the printing out of those works on paper or their storage on a USB stick.

51. As is clear from paragraph 40 and 42 of the present judgment, the limitation laid down in Article 5(3)(n) of Directive 2001/29 covers, in principle, only certain acts of communication normally falling under the exclusive right of the author provided for in Article 3 of that directive, namely those by which the establishments in question make a work available to individual members of the public, for the purpose of research or private study, by dedicated terminals installed on their premises.

52. It is undisputed that acts such as the printing out of a work on paper or its storage on a USB stick, even if made possible by the specific features of the dedicated terminals on which that
work can be consulted, are not acts of ‘communication’, within the meaning of Article 3 of Directive 2001/29, but rather of ‘reproduction’, within the meaning of Article 2 of that directive.

53 What is involved is the creation of a new analogue or digital copy of the work that an establishment makes available to users by means of dedicated terminals.

54 Such acts of reproduction, unlike some operations involving the digitisation of a work, also cannot be permitted under an ancillary right stemming from the combined provisions of Articles 5(2)(c) and 5(3)(n) of Directive 2001/29, since they are not necessary for the purpose of making the work available to the users of that work, by dedicated terminals, in accordance with the conditions laid down by those provisions. Moreover, since those acts are carried out not by the establishments referred to in Article 5(3)(n) of Directive 2001/29, but rather by the users of the dedicated terminals installed within those establishments, they cannot be authorised under that provision.

55 By contrast, such acts of reproduction on analogue or digital media may, if appropriate, be authorised under the national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of Directive 2001/29, since, in each individual case, the conditions laid down by those provisions, in particular as regards the fair compensation which the rightholder must receive, are met.

56 Furthermore, such acts of reproduction must observe the conditions set out in Article 5(5) of Directive 2001/29. Consequently, the extent of the texts reproduced may not, in particular, unreasonably prejudice the legitimate interests of the rightholder.

57 Having regard to the foregoing considerations, the answer to the third question is that Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that directive provided that, in each individual case, the conditions laid down by those provisions are met.

(…)

On those grounds, the Court (Fourth Chamber) hereby rules:

1. The concept of ‘purchase or licensing terms’ provided for in Article 5(3)(n) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be understood as requiring that the rightholder and an establishment, such as a publicly accessible library, referred to in that provision must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use that work.

2. Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

3. Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that directive provided that, in each individual case, the conditions laid down by those provisions are met.
Preamble

The Parties to this Convention, signatories hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are common to its members;

Noting the continued development of information and communication technology and the numerous international initiatives and their impact at a European and international level;

Recognising the cross-border nature of interactive services that are diffused on-line by new means of electronic communication and their growing importance in facilitating the economic, social and cultural progress of the Council of Europe member States;

Recalling the system established by the legislation of the European Community for the exchange of the texts of draft domestic regulations concerning “Information Society Services”;

Noting the need for all Council of Europe member States to be kept regularly informed of legislative developments on “Information Society Services” at a Pan-European level and, where necessary, to have the possibility to discuss and exchange information and ideas regarding these developments;

Agreeing on the desirability to provide a legal framework to enable member States of the Council of Europe to exchange, where practicable by electronic means, texts of draft domestic regulations aimed specifically at “Information Society Services”,

Have agreed as follows:

Article 1 – Object and scope of application

1. In accordance with the provisions of this Convention, the Parties shall exchange texts, where practicable by electronic means, of draft domestic regulations aimed specifically at “Information Society Services” and shall co-operate in the functioning of the information and legal co-operation system set up under the Convention.

2. This Convention shall not apply:

a. to domestic regulations which are exempted from prior notification by virtue of European Community legislation (hereinafter referred to as “Community law”), or

b. where a notification has to be made to comply with other international agreements.

3. This Convention shall not apply:

a. to radio broadcasting services;

b. to television programme services covered by the European Convention on Transfrontier Television, opened for signature in Strasbourg on 5 May 1989 (ETS No. 132), as amended by the Protocol of 1 October 1998 (ETS No. 171);

c. to domestic regulations relating to matters which are covered by European Community legislation or international agreements in the fields of telecommunications services and financial services.

Article 2 – Definitions

For the purposes of this Convention:

a. “Information Society Services” means any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of a service;

b. “domestic regulations” means legal texts concerning the compliance with requirements of a general nature relating to the taking up and pursuit of service activities within the meaning of paragraph a of this article, in particular provisions concerning the service provider, the services and the recipient of services, excluding any rules which are not specifically aimed at the Information Society Services.

Article 3 – Receiving and transmitting authorities

Each Party shall designate an authority that is in charge of transmitting and receiving, where practicable by electronic means, draft domestic regulations aimed specifically at “Information Society Services” as well as any other documents pertaining to the functioning of the present Convention.

Article 4 – Procedure

1. Each Party shall transmit, where practicable by electronic means, the texts of draft domestic regulations which are aimed specifically at “Information Society Services” and which are at a stage of preparation in which it is still possible for them to be substantially amended, as well as a short summary of these texts in English or French. The Parties shall communicate the draft again under the above conditions if they make changes to the draft that have the effect of significantly altering its scope, shortening the timetable originally envisaged for implementation, adding specifications or requirements, or making the latter more restrictive.

2. Upon receipt of the texts of the draft domestic regulations and summaries under paragraph 1 above or paragraph 6 below, the Secretary General of the Council of Europe shall transmit them, where practicable by electronic means, to the authority of each Party.

3. Upon receipt of the texts and summaries under paragraph 2 above, each Party may transmit, where practicable by electronic means, observations on the texts of the draft domestic regulations in English or French to the Secretary General of the Council of Europe and to the Party concerned.

4. A Party receiving the observations under paragraph 3 above shall endeavour to take them into account as far as possible when preparing new domestic regulations.

5. Paragraphs 1 to 4 above shall not apply:

a. in cases where, for urgent reasons, occasioned by serious and unforeseeable circumstances relating to the protection of public health or safety, the protection of animals or the preservation of plants, and public policy, notably the protection of minors, a Party is obliged to prepare technical regulations in a very short space of time in order to enact and introduce them immediately without any consultations being possible;
b in cases where for urgent reasons occasioned by serious circumstances relating to the protection of the security and the integrity of the financial system, notably the protection of depositors, investors and insured persons, a Party is obliged to enact and to implement rules on financial services immediately;

in the cases mentioned in sub-paragraphs a and b, the Party shall give reasons to the Secretary General of the Council of Europe for the urgency of the measures in question;

c) domestic regulations enacted by or for regulated markets or by or for other markets or bodies carrying out clearing or settlement functions for those markets.

6 Each Party which finalises any domestic regulations aimed specifically at "Information Society Services" shall transmit the definitive text to the Secretary General of the Council of Europe without delay and where practicable by electronic means.

7 Upon receipt of the texts of the adopted domestic regulations under paragraph 6 above, the Secretary General of the Council of Europe shall make them available, where practicable by electronic means, and shall keep this information in a single database within the Council of Europe.

Article 5 – Declarations

The authorities referred to in Article 3 shall be designated by means of a declaration addressed to the Secretary General of the Council of Europe when the State concerned or the European Community becomes a Party to the present Convention in accordance with the provisions of Articles 8 and 9. Any change shall likewise be declared to the Secretary General of the Council of Europe.

Article 6 – Relationship to other instruments and agreements

1 This Convention shall not affect any international instrument which is binding on the Parties and which contains provisions on matters governed by this Convention.

2 The European Community shall equally fulfil the obligation to notify the texts transmitted to it by its member States in pursuance of the provisions of paragraph 1 of Article 4, and shall transmit to them the observations received by the other Parties, in pursuance of the provisions of paragraph 3 of Article 4.

Article 7 – Amendments to Article 1 of the Convention concerning excluded matters

1 Any amendment to Article 1, paragraph 3 of this Convention proposed by a Party shall be communicated to the Secretary General of the Council of Europe who shall forward the communication to the European Committee on Legal Cooperation (CDCJ).

2 The proposed amendment shall be examined by the Parties, which may adopt it by a two-thirds majority of the votes cast. The text adopted shall be forwarded to the Parties. The European Community shall have the same number of votes as the number of its member States.

3 On the first day of the month following the expiration of a period of four months after its adoption by the Parties, unless the Parties have notified objections by one-third of the votes cast, any amendment shall enter into force for those Parties which have not notified objection.

4 A Party which has notified an objection in pursuance of the provisions of paragraph 3 of Article 7 may subsequently withdraw it in whole or in part. Such withdrawal shall be made by means of a notification addressed to the Secretary General of the Council of Europe and shall become effective as from the date of its receipt.

Article 8 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe, the non-member States which have participated in its elaboration and the European Community. Such States and the European Community may express their consent to be bound by:

a signature without reservation as to ratification, acceptance or approval, or
b signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five signatories, of which at least one is not a member State of the European Economic Area, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraph 1.

4 In respect of any signatory which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of their consent to be bound by the Convention in accordance with the provisions of paragraph 2.

Article 9 – Accession to the Convention

1 After the entry into force of the present Convention, the Committee of Ministers of the Council of Europe, after consulting the Parties to the Convention, may invite any non-member State of the Council which has not participated in its elaboration to accede to this Convention, by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Parties entitled to sit on the Committee.

2 In respect of any State acceding to it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 10 – Reservations

No reservation may be made in respect of any provision of this Convention.

Article 11 – Territorial application

1 Any State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any Party may, at any later date, by declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory or territories specified in the declaration and for whose international relations it is responsible or on whose behalf it is authorised to give undertakings. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3 Any declaration made in pursuance of the preceding paragraph may, in respect of any territory mentioned in such declaration, be withdrawn by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 12 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 13 – Notification
The Secretary General of the Council of Europe shall notify the member States of the Council and any other signatories and parties to this Convention of:

- any signature;
- the deposit of any instrument of ratification, acceptance, approval or accession;
- any declaration made in pursuance of the provisions of Article 5;
- any notification received in pursuance of the provisions of Article 7;
- any date of entry into force of this Convention, in accordance with Articles 8, 9 and 11;
- any declaration received in pursuance of the provisions of paragraphs 2 and 3 of Article 11;
- any notification received in pursuance of the provision of paragraph 1 of Article 12;
- any other act, notification or communication relating to this Convention.


**THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,**

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof;

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

1. The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples.

2. The development of electronic commerce within the information society offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet.

3. Community law and the characteristics of the Community legal order are a vital asset to enable European citizens and operators to take full advantage, without consideration of borders, of the opportunities afforded by electronic commerce; this Directive therefore has the purpose of ensuring a high level of Community legal integration in order to establish a real area without internal borders for information society services.

4. It is important to ensure that electronic commerce could fully benefit from the internal market and therefore that, as with Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities(4), a high level of Community integration is achieved.

5. The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services; these obstacles arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas, obstacles might be justified in the light of the case-law of the Court of Justice of the European Communities; legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State.

6. In the light of Community objectives, of Articles 43 and 49 of the Treaty and of secondary Community law, these obstacles should be eliminated by coordinating certain national laws and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market; by dealing only with certain specific matters which give rise to problems for the internal market, this Directive is fully consistent with the need to respect the principle of subsidiarity as set out in Article 5 of the Treaty.

7. In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.

8. The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such.

9. The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

10. In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the protection of public health; according to Article 152 of the Treaty, the protection of public health is an essential component of other Community policies.

11. This Directive is without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts; amongst others, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(5) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection

(12) It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not preclude any incentive that might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed on a large number of the services covered by this Directive, must be excluded from the scope of this Directive.

(13) This Directive does not aim to establish rules on fiscal obligations nor does it pre-empt the drawing up of Community instruments concerning fiscal aspects of electronic commerce.

(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(19) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(20) which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks through the Internet.

(15) The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.

(16) The exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value; this does not cover promotional competitions or games where the purpose is to encourage the sale of goods or services at a lower price, if they arise, serve only to acquire the promoted goods or services.

(17) The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(21) and in Directive 98/84/EC of the European Parliament and of the Council of 21 October 1998 on the protection of services based on, or consisting of, conditional access(22); this definition covers any service normally provided for remuneration, at a distance, by means of a computer network, equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service; those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition.

(18) Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive 89/552/EEC and radio broadcasting are not information society services because they are not provided at individual request; contracts, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the signature of a contract or the examination of medical records or of company accounts or medical advice requiring the physical examination of a patient are not information society services.

(19) The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual presence of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled when a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its
economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.

(20) The definition of "recipient of a service" covers all types of usage of information society services, both by persons who provide information on open networks such as the Internet, and by persons who seek information on the Internet for private or professional reasons.

(21) The scope of the coordinated field is without prejudice to future Community harmonisation relating to information society services and to future legislation adopted at national level in accordance with Community law; the coordinated field covers only requirements relating to on-line activities such as on-line information, on-line advertising on-line shopping, on-line contracting and does not concern Member States’ legal requirements relating to goods such as safety standards, labelling obligations, or liability for goods, or Member States’ requirements relating to the delivery or the transport of goods, including the distribution of medicinal products; the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

(22) Information society services should be supervised at the societal level, in order to achieve an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the service originates; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.

(23) This Directive neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts; provisions of the applicable law designated by rules of private international law must not restrict the freedom to provide information society services as established in this Directive.

(24) In the context of this Directive, notwithstanding the rule on the control at source of information society services, it is legitimate under the conditions established in this Directive for Member States to take measures to restrict the free movement of information society services.

(25) National courts, including civil courts, dealing with private law disputes can take measures to derogate from the freedom to provide information society services in conformity with conditions established in this Directive.

(26) Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission.

(27) This Directive, together with the future Directive of the European Parliament and of the Council on distance marketing of consumer financial services, contributes to the creating of a legal framework for the on-line provision of financial services; this Directive does not pre-empt future initiatives in the area of financial services in particular with regard to the harmonisation of rules of conduct in this field; the possibility for Member States, established in this Directive, under certain circumstances of restricting the freedom to provide information society services in order to protect consumers also covers measures in the area of financial services in particular measures aiming at protecting investors.

(28) The Member States’ obligation not to subject access to the activity of an information society service provider to prior authorisation does not concern postal services covered by Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service; the physical delivery of a printed electronic mail message and does not affect voluntary accreditation systems, in particular for providers of electronic signature certification services.

(29) Commercial communications are essential for the financing of information society services and for developing a wide variety of new, charge-free services; in the interests of consumer protection and the harmonisation of commercial communications, including discounts, promotional offers and promotional competitions or games, must meet a number of transparency requirements; these requirements are without prejudice to Directive 97/7/EC; this Directive should not affect existing Directives on commercial communications, in particular Directive 98/43/EC.

(30) The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; the question of consent by recipient of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed by the Commission, by Directive 97/66/EC; in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communications are clearly identifiable as such in order to improve transparency and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

(31) Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent of the recipient by service providers established in their territory have to ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

(32) In order to remove barriers to the development of cross-border services within the Community which members of the regulated professions might offer on the Internet, it is necessary that compliance be guaranteed at Community level with professional rules aiming, in particular, to protect consumers or public health; codes of conduct at Community level would be the best means of determining the rules on the coordination of Member States’ legal requirements applicable to commercial communication; the drawing-up or, where appropriate, the adaptation of such rules should be encouraged without prejudice to the autonomy of professional bodies and associations.

(33) This Directive complements Community law and national law relating to regulated professions maintaining a coherent set of applicable rules in this field.

(34) Each Member State is to amend its legislation containing requirements, and in particular requirements as to form, which are likely to curb the use of contracts by electronic means; the examination of the legislation concerning such contracts should be systematic and should cover all the necessary stages and acts of the contractual process, including the filing of the contract; the result of this amendment should be to make contracts concluded electronically workable; the legal effect of electronic signatures is dealt with by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; the acknowledgement of receipt by a service provider may take the form of the on-line provision of the service paid for.

(35) This Directive does not affect Member States’ possibility of maintaining or establishing general or specific legal requirements for contracts which can be fulfilled by electronic
means, in particular requirements concerning secure electronic signatures.

(36) Member States may maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities, or professions exercising public authority; this possibility also covers contracts which require the involvement of courts, public authorities, or professions exercising public authority in order to have an effect with regard to third parties as well as contracts requiring by law certification or attestation by a notary.

(37) Member States’ obligation to remove obstacles to the use of electronic contracts concerns only obstacles resulting from legal requirements and not practical obstacles resulting from the impossibility of using electronic means in certain cases.

(38) Member States’ obligation to remove obstacles to the use of electronic contracts is to be implemented in conformity with legal requirements for contracts enshrined in Community law.

(39) The exceptions to the provisions concerning the contracts concluded exclusively by electronic mail or by equivalent individual communications provided for by this Directive, in relation to information to be provided and the placing of orders, should not enable, as a result, the bypassing of those provisions by providers of information society services.

(40) Both existing and emerging disparities in Member States’ legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

(41) This Directive strikes a balance between the different interests involved and establishes principles upon which industry agreements and standards can be based.

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" as a result cannot benefit from the liability exemptions established for these activities.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or public authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose for a similar time scale; this Directive does not affect Member States’ possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring, service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

(49) Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

(50) It is important that the proposed directive on the harmonisation of certain aspects of copyright and related rights in the information society and this Directive come into force within a similar time scale with a view to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and related rights infringements at Community level.

(51) Each Member State should be required, where necessary, to amend any legislation which is liable to hamper the use of schemes for the out-of-court settlement of disputes through electronic channels; the result of this amendment must be to make the functioning of such schemes genuinely and effectively possible in law and in practice, even across borders.

(52) The effective exercise of the freedoms of the internal market makes it necessary to guarantee victims of online actions access to means of settling disputes; damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; Member States should examine the need to provide access to judicial procedures by appropriate electronic means.

(53) Directive 96/27/EC, which is applicable to information society services, provides a mechanism relating to actions for an injunction aimed at the protection of the collective interests of consumers; this mechanism will contribute to the free movement of information society services by ensuring a high level of consumer protection.

(54) The sanctions provided for under this Directive are without prejudice to the possibility of criminal sanctions for infringement of national provisions under national law; Member States are not obliged to provide criminal sanctions for infringement of national provisions adopted pursuant to this Directive.

(55) This Directive does not affect the law applicable to contractual obligations relating to consumer contracts; accordingly, this Directive cannot have the result of depriving
the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence.

(58) As regards the derogation contained in this Directive regarding contractual obligations concerning contracts concluded by consumers, those obligations should be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract.

(57) The Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

(59) This Directive should not apply to services supplied by service providers established in a third country, in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitrals) on legal issues.

(60) Despite the global nature of electronic communications, coordination of national regulatory measures at European Union level is necessary in order to avoid fragmentation of the internal market, and for the establishment of an appropriate European regulatory framework; such coordination should also contribute to the establishment of a common and strong negotiating position in international forums.

(61) In order to allow the unhampered development of electronic commerce, the legal framework must be clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.

(62) Cooperation with third countries should be strengthened in the area of electronic commerce, in particular with applicant countries, the developing countries and the European Union’s other trading partners. Cooperation of an appropriate level should be strengthened with these countries, in particular in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible.

(63) The adoption of this Directive will not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society; in particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens have access to the cultural European heritage provided in the digital environment.

(64) Electronic communication offers the Member States an excellent means of providing public services in the cultural, educational and linguistic fields.

(65) The Council, in its resolution of 19 January 1999 on the consumer dimension of the information society[25], stressed that the protection of consumers deserved special attention in this field; the Commission will examine the degree to which existing consumer protection rules provide insufficient protection in the context of the information society and will identify, where necessary, the deficiencies of this legislation and those issues which could require additional measures; if need be, the Commission should make specific additional proposals to resolve such deficiencies that will thereby have been identified.

HAY ADOPTED THIS DIRECTIVE.

CHAPTER I GENERAL PROVISIONS

Article 1 Objective and scope

1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary, the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlement, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.

5. This Directive shall not apply to:
   (a) the field of taxation;
   (b) questions relating to information society services covered by Directives 95/14/EC and 97/66/EC;
   (c) questions relating to agreements or practices governed by cartel law;
   (d) the following activities of information society services:
      - the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
      - the representation of a client and defence of his interests before the courts,
      - gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Article 2 Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:

(a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
(b) "service provider": any natural or legal person providing an information society service;
(c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;
(d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;
(e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;
(f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:
- information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,
- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;


(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:
- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,
- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;

(ii) The coordinated field does not cover requirements such as:
- requirements applicable to goods as such,
- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

Article 3 Internal market
1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.

2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.

3. Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.

4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:

(a) the measures shall be:

(i) necessary for one of the following reasons:
- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons, - the protection of public health,
- public security, including the safeguarding of national security and defence,
- the protection of consumers, including investors;

(ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;

(iii) proportionate to those objectives;

(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:

- asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,
- notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.

5. Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.

6. Without prejudice to the Member State's possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.

CHAPTER II PRINCIPLES

Section 1: Establishement and information requirements

Article 4 Principle excluding prior authorisation

1. Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect.

2. Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services(28).

Article 5 General information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions:
- any professional body or similar institution with which the service provider is registered,
- the professional title and the Member State where it has been granted,
- a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29).

2. In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

Section 2: Commercial communications

Article 6 Information to be provided
In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

(a) the commercial communication shall be clearly identifiable as such;
(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7 Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Article 8 Regulated professions

1. Member States shall ensure that the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.

2. Without prejudice to the autonomy of professional bodies and associations, Member States and the Commission shall encourage professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication in conformity with the rules referred to in paragraph 1

3. When drawing up proposals for Community initiatives which may become necessary to ensure the proper functioning of the Internal Market with regard to the information referred to in paragraph 2, the Commission shall take due account of codes of conduct applicable at Community level and shall act in close cooperation with the relevant professional associations and bodies.

4. This Directive shall apply in addition to Community Directives concerning access to, and the exercise of, activities of the regulated professions.

Section 3: Contracts concluded by electronic means

Article 9 Treatment of contracts

1. Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

2. Member States may lay down that paragraph 1 shall not apply to all or certain contracts falling into one of the following categories:

(a) contracts that create or transfer rights in real estate, except for rental rights;
(b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;
(c) contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;
(d) contracts governed by family law or by the law of succession.

3. Member States shall indicate to the Commission the categories referred to in paragraph 2 to which they do not apply paragraph 1. Member States shall submit to the Commission every five years a report on the application of paragraph 2 explaining the reasons why they consider it necessary to maintain the category referred to in paragraph 2(b) to which they do not apply paragraph 1.

Article 10 Information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

(a) the different technical steps to follow to conclude the contract;
(b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
(c) the technical means for identifying and correcting input errors prior to the placing of the order;
(d) the languages offered for the conclusion of the contract.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

3. Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

4. Paragraphs 1 and 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Article 11 Placing of the order

1. Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

- the service provider has to acknowledge the receipt of the recipient’s order without undue delay and by electronic means,
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

3. Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Section 4: Liability of intermediary service providers

Article 12 "Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 "Caching"
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
   (a) the provider does not modify the information;
   (b) the provider complies with conditions on access to the information;
   (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
   (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
   (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
   (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 No general obligation to monitor
1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

CHAPTER III IMPLEMENTATION

Article 16 Codes of conduct
1. Member States and the Commission shall encourage:
   (a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;
   (b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;
   (c) the accessibility of these codes of conduct in the Community languages by electronic means;
   (d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;
   (e) the drawing up of codes of conduct regarding the protection of minors and human dignity.
2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.

Article 17 Out-of-court dispute settlement
1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.
2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.
3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

Article 18 Court actions
1. Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.
2. The Annex to Directive 98/27/EC shall be supplemented as follows:


Article 19 Cooperation
1. Member States shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure that service providers supply them with the requisite information.
2. Member States shall cooperate with other Member States; they shall, to that end, appoint one or several contact points, whose details they shall communicate to the other Member States and to the Commission.

3. Member States shall, as quickly as possible, and in conformity with national law, provide the assistance and information requested by other Member States or by the Commission, including by appropriate electronic means.

4. Member States shall establish contact points which shall be accessible at least by electronic means and from which recipients and service providers may:
   (a) obtain general information on contractual rights and obligations as well as on the complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;
   (b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.

5. Member States shall encourage the communication to the Commission of any significant administrative or judicial decisions taken in their territory regarding disputes relating to information society services and practices, usage and customs relating to electronic commerce. The Commission shall communicate these decisions to the other Member States.

Article 20
Sanctions
Member States shall determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are enforced. The sanctions they provide for shall be effective, proportionate and dissuasive.

CHAPTER IV FINAL PROVISIONS
Article 21 Re-examination
1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, "notice and take down" procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

Article 22 Transposition
1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 17 January 2002. They shall forthwith inform the Commission thereof.

2. When Member States adopt the measures referred to in paragraph 1, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The methods of making such reference shall be laid down by Member States.

Article 23
Entry into force
This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 24
Addressees
This Directive is addressed to the Member States.

Done at Luxemburg, 8 June 2000.

For the European Parliament
The President
N. Fontaine
For the Council
The President
G. d’Oliveira Martins
(1) OJ C 30, 5.2.1999, p. 4.
(2) OJ C 169, 16.6.1999, p. 36.

ANNEX
DEROGATIONS FROM ARTICLE 3
As provided for in Article 3(3), Article 3(1) and (2) do not apply to:
- copyright, neighbouring rights, rights referred to in Directive 87/56/EEC(1) and Directive 96/93/EC(2) as well as industrial property rights,
- the emission of electronic money by institutions in respect of which Member States have applied one of the derogations provided for in Article 8(1) of Directive 2000/46/EC(3).
- the permissibility of unsolicited commercial communications by electronic mail.
(3) Not yet published in the Official Journal.

Relevant Case law concerning directive 2000/31/EC

Case C-324/09, L’Oréal SA and others v. eBay International AG and others

26 L’Oréal is a manufacturer and supplier of perfumes, cosmetics and hair-care products. In the United Kingdom it is the proprietor of a number of national trade marks. It is also the proprietor of Community trade marks.

27 L’Oréal operates a closed selective distribution network, in which authorised distributors are restrained from supplying products to other distributors. eBay operates an electronic marketplace on which are displayed listings of goods offered for sale by persons who have registered for that purpose with eBay and have created a seller’s account with it. eBay charges a percentage fee on completed transactions.

29 eBay enables prospective buyers to bid for items offered by sellers. It also allows items to be sold without an auction, and thus for a fixed price, by means of a system known as ‘Buy It Now’. Sellers can also set up online shops on eBay sites. An online shop lists all the items offered for sale by one seller at a given time.

30 Sellers and buyers must accept eBay’s online-market user agreement. One of the terms of that agreement is a prohibition on selling counterfeit items and on infringing trade marks.

31 In some cases eBay assists sellers in order to enhance their offers for sale, to set up online shops, to promote and increase their sales. It also advertises some of the products sold on its marketplace using search engine operators such as Google to trigger the display of advertisements.

32 On 22 May 2007, L’Oréal sent eBay a letter expressing its concerns about the widespread incidence of transactions infringing its intellectual property rights on eBay’s European websites.

33 L’Oréal was not satisfied with the response it received and brought actions against eBay in various Member States, including an action before the High Court of Justice (England & Wales), Chancery Division.

34 L’Oréal’s action before the High Court of Justice sought a ruling, first, that eBay and the individual defendants are liable for sales of 17 items made by those individuals through the website www.ebay.co.uk. L’Oréal claiming that those sales infringed the rights conferred on it by, inter alia, the figurative Community trade mark including the words ‘Amor Amor’ and the national word mark ‘Lancôme’.

35 It is common ground between L’Oréal and eBay that two of those 17 items are counterfeit goods bearing L’Oréal trade marks.

36 Although L’Oréal does not claim that the other 15 items are counterfeit, it none the less considers that the sale of the items infringed its trade mark rights, since those items were either goods that were not intended for sale (such as tester or drumming products) or goods bearing L’Oréal trade marks intended for sale in North America and not in the European Economic Area (‘EEA’). Furthermore, some of the items were sold without packaging.

37 Whilst refraining from ruling at this stage on the question as to the extent to which L’Oréal’s trade mark rights have been infringed, the High Court of Justice has confirmed that the individual defendants made the sales described by L’Oréal on the website www.ebay.co.uk.

38 Second, L’Oréal submits that eBay is liable for the use of L’Oréal’s trade marks where those marks are displayed on eBay’s website and where sponsored links triggered by the use of keywords corresponding to the trade marks are displayed on the websites of search engine operators, such as Google.

39 Concerning the last point, it is not disputed that eBay, by choosing keywords corresponding to L’Oréal trade marks in Google’s ‘Ad Words’ referencing service, caused to be displayed, each time that there was a match between a keyword and the word entered in Google’s search engine by an internet user, a sponsored link to the site www.ebay.co.uk. That link would appear in the ‘sponsored links’ section displayed on either the right-hand side, or on the upper part, of the screen displayed by Google.

40 Thus, on 27 March 2007, when an internet user entered the words ‘shu uemura’ – which in essence coincide with L’Oréal’s national word mark ‘Shu Uemura’ – as a search string in the Google search engine, the following eBay advertisement was displayed in the ‘sponsored links’ section: ‘Shu Uemura Great deals on Shu uemura Shop on eBay and Save! www.ebay.co.uk’.

41 Clicking on that sponsored link led to a page on the www.ebay.co.uk website which showed ‘96 items found for shu uemura’. Most of those items were expressly stated to be from Hong Kong.

42 Similarly, taking one of the other examples, when, on 27 March 2007, an internet user entered the words ‘matrix hair’, which correspond in part to L’Oréal’s national word mark ‘Matrix’, as a search string in the Google search engine, the following eBay listing was displayed as a ‘sponsored link’: ‘Matrix hair Fantastic low prices here Feed your passion on ebay.co.uk/ www.ebay.co.uk’.

43 Third, L’Oréal has claimed that, even if eBay was not liable for the infringements of its trade mark rights, it should be granted an injunction against eBay by virtue of Article 11 of Directive 2004/48.

44 L’Oréal reached a settlement with some of the individual defendants (Mr Potts, Ms Ratchford, Ms Ormsby, Mr Garke and Ms Clarke) and obtained judgment in default against the others (Mr Fox and Ms Bi). Subsequently, in March 2009, a hearing dealing with the action against eBay was held before the High Court of Justice.

45 By judgment of 22 May 2009, the High Court of Justice made a number of findings of fact and concluded that the state of the proceedings did not permit final judgment in the case, as a number of questions of law first required an interpretation from the Court of Justice of the European Union.
In its judgment, the High Court of Justice notes that eBay has installed filters in order to detect listings which might contravene the conditions of use of the site. That court also notes that eBay has developed, using a programme called VeRO (Verified Rights Owner), a notice and take-down system that is intended to provide intellectual property owners with assistance in removing infringing listings from the marketplace. L’Oréal has declined to participate in the VeRO programme, contending that the programme is unsatisfactory.

47 The High Court of Justice has also stated that eBay applies sanctions, such as the temporary – or even permanent – suspension of sellers who have contravened the conditions of use of the online marketplace.

48 Despite the findings set out above, the High Court of Justice took the view that eBay could do more to reduce the number of sales on its online marketplace which infringe intellectual property rights. According to that court, eBay could use additional filters. It could also include in its rules a prohibition on selling, without the consent of the trade mark proprietors, trade-marked goods originating from outside the EEA. It could also impose additional restrictions on the volumes of products that can be listed at any one time and apply sanctions more rigorously.

49 The High Court of Justice states, however, that the fact that it would be possible for eBay to do more does not necessarily mean that it is legally obliged to do so.

50 By decision of 16 July 2009, which follows on from the judgment of 22 May 2009, the High Court of Justice decided to stay the proceedings and refer the following questions to the Court for a preliminary ruling:

(1) Where perfume and cosmetic testers (i.e. samples for use in demonstrating products to consumers in retail outlets) and dramming bottles (i.e. containers from which small aliquots can be taken for supply to consumers as free samples) which are not intended for sale to consumers (and are often marked “not for sale” or “not for individual sale”) are supplied without charge to the trade mark proprietor’s authorised distributors, are such goods “put on the market” within the meaning of Article 7(1) of [Directive 89/104] and Article 13(1) of [Regulation No 40/94]? (2) Where the boxes (or other outer packaging) have been removed from perfumes and cosmetics without the consent of the trade mark proprietor, does this constitute a “legitimate reason” for the trade mark proprietor to oppose further commercialisation of the unboxed products within the meaning of Article 7(2) of [Directive 89/104] and Article 13(2) of [Regulation No 40/94]? (3) Does it make a difference to the answer to question 2 above if:

(a) as a result of the removal of the boxes (or other outer packaging), the unboxed products do not bear the information required by Article 6(1) of [Directive 76/768], and in particular do not bear a list of ingredients or a “best before date”?

(b) as a result of the absence of such information, the offer for sale or sale of the unboxed products constitutes a criminal offence according to the law of the Member State of the Community in which they are offered for sale or sold by third parties?

(4) Does it make a difference to the answer to question 2 above if the further commercialisation damages, or is likely to damage, the image of the goods and hence the reputation of the trade mark? If so, is that effect to be presumed, or is it required to be proved by the trade mark proprietor?

(5) Where a trader which operates an online marketplace purchases the use of a sign which is identical to a registered trade mark as a keyword from a search engine operator so that the sign is displayed to a user by the search engine in a sponsored link to the website of the operator of the online marketplace, does the display of the sign in the sponsored link constitute “use” of the sign within the meaning of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94]? (6) Where clicking on the sponsored link referred to in question 5 above leads the user directly to advertisements or offers for sale of goods identical to those for which the trade mark is registered under the sign placed on the website by other parties, some of which infringe the trade mark and some of which do not infringe the trade mark by virtue of the differing statuses of the respective goods, does that constitute use of the sign by the operator of the online marketplace “in relation to” the infringing goods within the meaning of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94]? (7) Where the goods advertised and offered for sale on the website referred to in question 6 above include goods which have not been put on the market within the EEA by or with the consent of the trade mark proprietor, is it sufficient for such use to fall within the scope of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94] and outside Article 7(1) of [Directive 89/104] and Article 13(1) of [Regulation No 40/94] that the advertisement or offer for sale is targeted at consumers in the territory covered by the trade mark or must the trade mark proprietor show that the advertisement or offer for sale necessarily entails putting the goods in question on the market within the territory covered by the trade mark?

(8) Does it make any difference to the answers to questions 5 to 7 above if the use complained of by the trade mark proprietor consists of the display of the sign on the website of the operator of the online marketplace itself rather than a sponsored link?

(9) If it is sufficient for such use to fall within the scope of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94] and outside Article 7(1) of [Directive 89/104] and Article 13 ... of [Regulation No 40/94] that the advertisement or offer for sale is targeted at consumers in the territory covered by the trade mark:

(a) does such use consist of or include “the storage of information provided by a recipient of the service” within the meaning of Article 14(1) of [Directive 2000/31]? (b) if the use does not consist exclusively of activities falling within the scope of Article 14(1) of [Directive 2000/31], but includes such activities, is the operator of the online marketplace exempted from liability to the extent that the use consists of such activities and if so may damages or other financial remedies be granted in respect of such use to the extent that it is not exempted from liability?

(c) in circumstances where the operator of the online marketplace has knowledge that goods have been advertised, offered for sale and sold on its website in infringement of registered trade marks, and that infringements of such registered trade marks are likely to continue to occur through the advertisement, offer for sale and sale of the same or similar goods by the same or different users of the website, does this constitute “actual knowledge” or “awareness” within the meaning of Article 14(1) of [Directive 2000/31]?

(10) Where the services of an intermediary such as an operator of a website have been used by a third party to infringe a registered trade mark, does Article 11 of [Directive 2004/48] require Member States to ensure that the trade mark proprietor can obtain an injunction against the intermediary to prevent further infringements of the said trade mark as opposed to continuation of that specific act of infringement, and if so what is the scope of the injunction that shall be made available? 

(...)

On those grounds, the Court (Grand Chamber) hereby rules:

1. Where goods located in a third State, which bear a trade mark registered in a Member State of the European Union or a Community trade mark and have not previously been put on the market in the European Economic Area or, in the case of a Community trade mark, in the European Union, (i) are sold by an economic operator on an online marketplace without the consent of the trade mark proprietor to a consumer located in
the territory covered by the trade mark or (ii) are offered for sale or advertised on such a marketplace targeted at consumers located in that territory, the trade mark proprietor may prevent that sale, offer for sale or advertising by virtue of the rules set out in Article 5 of First Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks, as amended by the Agreement on the European Economic Area of 2 May 1992, or in Article 9 of Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark. It is the task of the national courts to assess on a case-by-case basis whether relevant factors exist, on the basis of which it may be concluded that an offer for sale or an advertisement displayed on an online marketplace accessible from the territory covered by the trade mark is targeted at consumers in that territory.

2. Where the proprietor of a trade mark supplies to its authorised distributors items bearing that mark, intended for demonstration to consumers in authorised retail outlets, and bottles bearing the mark from which small quantities can be taken for supply to consumers as free samples, those goods, in the absence of any evidence to the contrary, are not put on the market within the meaning of Directive 89/104 and Regulation No 40/94.

3. Article 5 of Directive 89/104 and Article 9 of Regulation No 40/94 must be interpreted as meaning that the proprietor of a trade mark may, by virtue of the exclusive right conferred by the mark, oppose the resale of goods such as those at issue in the main proceedings, on the ground that the person reselling the goods has removed their packaging, where the consequence of that removal is that essential information, such as information relating to the identity of the manufacturer or the person responsible for marketing the cosmetic product, is missing. Where the removal of the packaging has not resulted in the absence of that information, the trade mark proprietor may nevertheless oppose the resale of an unboxed perfume or cosmetic product bearing his trade mark, if he establishes that the removal of the packaging has damaged the image of the product and, hence, the reputation of the trade mark.

4. On a proper construction of Article 5(1)(a) of Directive 89/104 and Article 9(1)(a) of Regulation No 40/94, the proprietor of a trade mark is entitled to prevent an online marketplace operator from advertising – on the basis of a keyword which is identical to his trade mark and which has been selected in an internet referencing service by that operator – goods bearing that trade mark which are offered for sale on the marketplace, where the advertising does not enable reasonably well-informed and reasonably observant internet users, or enables them only with difficulty, to ascertain whether the goods come from the proprietor of the trade mark or from an undertaking economically linked to that proprietor or, on the contrary, originate from a third party.

5. The operator of an online marketplace does not ‘use’ – for the purposes of Article 5 of Directive 89/104 or Article 9 of Regulation No 40/94 – signs identical with or similar to trade marks which appear in offers for sale displayed on its site.

6. Article 14(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) must be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored. The operator plays such a role when it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them. Where the operator of the online marketplace has not played an active role within the meaning of the preceding paragraph and the service provided falls, as a consequence, within the scope of Article 14(1) of Directive 2000/31, the operator none the less cannot, in a case which may result in an order to pay damages, rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31/EC.

7. The third sentence of Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as requiring the Member States to ensure that the national courts have jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade.

Joined Cases C-236/08 to C-238/08: Google France SARL, Google Inc. vs. Louis Vuitton Malletier SA (C-236/08), Google France SARL vs. Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL vs Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08)

1. An internet referencing service provider that stores, as a keyword, a sign identical to a trade mark and organises the display of advertisements on the basis of that keyword does not use that sign within the meaning of Article 5(1) and (2) of Directive 89/104 relating to trade marks or of Article 9(1) of Regulation No 40/94 on the Community trade mark.

It is common ground that the referencing service provider carries on a commercial activity with a view to economic advantage when it stores as keywords, for certain of its clients, signs which are identical with trade marks and arranges for the display of ‘ads’ on the basis of those keywords. It is also common ground that that service is not supplied only to the proprietors of those trade marks or to operators entitled to market their goods or services, but is provided without the consent of the proprietors and is supplied to their competitors or to imitators.

Although it is clear from those factors that the referencing service provider operates ‘in the course of trade’ when it permits advertisers to select, as keywords, signs identical to trade marks, stores those signs and displays its clients’ ‘ads’ on the basis thereof, it does not follow, however, from those factors that that service provider itself ‘uses’ those signs within the terms of Article 5 of Directive 89/104 and Article 9 of Regulation No 40/94.

The use, by a third party, of a sign identical or similar to the proprietor’s trade mark implies, at the very least, that that third party uses the sign in its own commercial communication. A referencing service provider allows its clients to use signs identical or similar to trade marks, without itself using those signs. That conclusion cannot be called into question by the fact that the service provider is paid by its clients for the use of those signs. The fact of creating the technical conditions necessary for the use of a sign and being paid for that service does not mean that the party offering the service itself uses the sign.

2. The use as a keyword by the advertiser of a sign identical to the trade mark of a competitor in an internet referencing service in order that internet users may become aware, not only of the goods or services offered by that competitor, but also of those of the advertiser, constitutes a use in relation to the goods or services of that advertiser. In addition, even in cases in which the advertiser does not seek, by its use, as a keyword, of a sign identical to the trade mark, to present its goods or services to internet users as an alternative to the goods or services of the proprietor of the trade mark but, on the contrary, seeks to mislead internet
users as to the origin of its goods or services by making them believe that they originate from the proprietor of the trade mark or from an undertaking economically connected to it, there is use 'in relation to goods or services'. Such use exists in any event when the third party uses the sign identical to the trade mark in such a way that a link is established between that sign and the goods marketed or the services provided by the third party. It follows that use by an advertiser of a sign identical with a trade mark as a keyword in the context of an internet referencing service falls within the concept of use 'in relation to goods or services' within the meaning of Article 5(1)(a) of Directive 89/104 relating to trade marks.

3. Article 5(1)(a) of Directive 89/104 relating to trade marks and Article 9(1)(a) of Regulation No 40/94 on the Community trade mark must be interpreted as meaning that the proprietor of a trade mark is entitled to prohibit an advertiser from advertising, on the basis of a keyword identical to that trade mark which that advertiser has, without the consent of the proprietor, selected in connection with an internet referencing service, goods or services identical to those for which that mark is registered, when that advertisement does not enable an average internet user, or enables that user only with difficulty, to ascertain whether the goods or services referred to therein originate from the proprietor of the trade mark or an undertaking economically connected to it or, on the contrary, originate from a third party.

In such a situation, which is, moreover, characterised by the fact that the 'ad' in question appears immediately after entry of the trade mark as a search term by the internet user concerned and is displayed at a point when the trade mark is, in its capacity as a search term, also displayed on the screen, the internet user may err as to the origin of the goods or services in question. In those circumstances, the use by the third party of the sign identical to the mark as a keyword triggering the display of that 'ad' is liable to create the impression that there is a material link in the course of trade between the goods or services in question and the proprietor of the trade mark.

Having regard to the essential function of a trade mark, which, in the area of electronic commerce, consists in particular in enabling internet users browsing the 'ads' displayed in response to a search relating to a specific trade mark to distinguish the goods or services of the proprietor of that mark from those of other economic operators if it wishes to ensure that its 'ad' appears before those of those operators which have also selected its mark as a keyword. Furthermore, even if the proprietor of the mark must, as necessary, agree to pay a higher price per click than that offered by third parties that have also selected that trade mark, the proprietor cannot be certain that its 'ad' will appear before those of those third parties, given that other factors are also taken into account in determining the order in which the ads are displayed. Nevertheless, those repercussions of use by third parties of a sign identical with the trade mark do not of themselves constitute an adverse effect on the advertising function of the trade mark.

5. Article 14 of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider when that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser’s activities, it failed to act expeditiously to remove or to disable access to the data concerned.

It is for the national court to assess, on a case-by-case basis, whether the facts of the dispute before it indicate adverse effects or a risk thereof, on the function of indicating origin. When a third party’s 'ad' suggests that there is an economic link between that third party and the proprietor of the trade mark, the conclusion must be that there is an adverse effect on the function of indicating origin. When the 'ad', while not suggesting the existence of an economic link, is to such an extent vague as to the origin of the goods or services at issue that normally informed and reasonably attentive internet users are unable to determine, on the basis of the advertising link and the commercial message attached thereto, whether the advertiser is a third party vis-à-vis the proprietor of the trade mark or, on the contrary, economically linked to that proprietor, the conclusion must also be that there is an adverse effect on that function of the trade mark.

4. Since the course of trade provides a varied offer of goods and services, the proprietor of a trade mark may have not only the objective of indicating, by means of that mark, the origin of its goods or services, but also that of using its mark for advertising purposes designed to inform and persuade consumers. Accordingly, the proprietor of a trade mark is entitled to prohibit a third party from using, without the proprietor’s consent, a sign identical with its trade mark in relation to goods or services which are identical to those for which that trade mark is registered, when that use adversely affects the proprietor’s use of its mark as a factor in sales promotion or as an instrument of commercial strategy.

With regard to the use by internet advertisers of a sign identical to another person’s trade mark as a keyword for the purposes of displaying advertising messages, it is clear that that use is liable to have certain repercussions on the advertising use of that mark by its proprietor and on the latter’s commercial strategy.

Having regard to the important position which internet advertising occupies in trade and commerce, it is plausible that the proprietor of a trade mark may register its own trade mark as a keyword with a referencing service provider in order to have an ‘ad’ appear under the heading ‘sponsored links’. Where that is the case, the proprietor of the mark must, as necessary, agree to pay a higher price per click than certain other economic operators if it wishes to ensure that its ‘ad’ appears before those of those operators which have also selected its mark as a keyword. Furthermore, even if the proprietor of the mark is prepared to pay a higher price per click than that offered by third parties that have also selected that trade mark, the proprietor cannot be certain that its ‘ad’ will appear before those of those third parties, given that other factors are also taken into account in determining the order in which the ads are displayed. Nevertheless, those repercussions of use by third parties of a sign identical with the trade mark do not of themselves constitute an adverse effect on the advertising function of the trade mark.

Case C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH.

11 Having established that a website was offering, without their agreement, either a download or 'streaming' of some of the films which they had produced, Constantin Film and Wega, two film production companies, referred the matter to the court responsible for hearing applications for interim measures with a view to obtaining, on the basis of Article 81(1)(a) of the UrhG, an order enjoining UPC Telekabel, an internet service provider, to block the access of its customers to the website at issue, inasmuch as that site makes available to the public, without their consent, cinematographic works over which they hold a right related to copyright.

12 By order of 13 May 2011, the Handelsgericht Wien (Commercial Court, Vienna) (Austria) prohibited UPC Telekabel from providing its customers with access to the website at issue; that prohibition was to be carried out in particular by blocking that site’s domain name and current IP ('Internet Protocol') address and any other IP address of that site of which UPC Telekabel might be aware.
13 In June 2011, the website at issue ceased its activity following an action of the German police forces against its operators.

14 By order of 27 October 2011, the Oberlandesgericht Wien (Higher Regional Court, Vienna) [Austria], as an appeal court, partially reversed the order of the court of first instance in so far as it had wrongly specified the means that UPC Telekabel had to introduce in order to block the website at issue and thus execute the injunction. In order to reach that conclusion, the Oberlandesgericht Wien first of all held that Article 8(1)(a) of the UrhG must be interpreted in the light of Article 8(3) of Directive 2001/29. It then held that, by giving its customers access to content illegally placed online, UPC Telekabel had to be regarded as an intermediary whose services were used to infringe a right related to copyright, with the result that Constantin Film and Wega were entitled to request that an injunction be issued against UPC Telekabel. However, as regards the protection of copyright, the Oberlandesgericht Wien held that UPC Telekabel could only be required, in the form of an obligation to achieve a particular result, to forbid its customers access to the website at issue, but that it had to remain free to decide the means to be used.

15 UPC Telekabel appealed on a point of law to the Oberster Gerichtshof (Supreme Court) [Austria].

16 In support of its appeal, UPC Telekabel submits inter alia that its services could not be considered to be used to infringe a copyright or related right within the meaning of Article 8(3) of Directive 2001/29 because it did not have any business relationship with the operators of the website at issue and it was not established that its own customers acted unlawfully. In any event, UPC Telekabel claims that the various blocking measures which may be introduced can all be technically circumvented and that some of them are excessively costly.

17 In those circumstances, the Oberster Gerichtshof decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

1. Is Article 8(3) of Directive 2001/29 ... to be interpreted as meaning that a person who makes protected subject-matter available on the internet without the rightholder's consent [for the purpose of Article 3(2) of Directive 2001/29] is using the services of the [internet] access providers of persons seeking access to that protected subject-matter?

If the answer to the first question is in the negative:

2. Are reproduction for private use [within the meaning of Article 5(2)(b) of Directive 2001/29] and transient and incidental reproduction [within the meaning of Article 5(1) of Directive 2001/29] permissible only if the original of the reproduction was lawfully reproduced, distributed or made available to the public?

If the answer to the first question or the second question is in the affirmative and an injunction is therefore to be issued against the user's [internet] access provider in accordance with Article 8(3) of Directive 2001/29?

3. Is it compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to prohibit in general terms an [internet] access provider from allowing its customers access to a certain website (thus without ordering specific measures) as long as the material available on that website is provided exclusively or predominantly without the rightholder's consent, if the access provider can avoid incurring coercive penalties for breach of the prohibition by showing that it had nevertheless taken all reasonable measures?

If the answer to the third question is in the negative:

4. Is it compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to require an [internet] access provider to take specific measures to make it more difficult for its customers to access a website containing material that is made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge?

(…)
that there have been cases in the Estonian courts where authors have been punished for the contents of a comment. Delfi prohibits comments the content of which does not comply with good practice. These are comments that:
- contain threats;
- contain insult;
- incite hostility and violence;
- incite illegal activities;
- contain obscene expressions and vulgarities.
Delfi has the right to remove such comments and restrict their author's access to the writing of comments.

The functioning of the notice-and-take-down system was also explained in the text.

11. The Government submitted that in Estonia Delfi had a notorious history of publishing defaming and degrading comments. Thus, on 22 September 2005 the weekly newspaper Eesti Ekspress had published a public letter from the editorial board to the Minister of Justice, the Chief Public Prosecutor and the Chancellor of Justice in which concern was expressed about incessant taunting of people on public websites in Estonia. Delfi was named as a source of brutal and arrogant mockery.

(a) Existence of an interference
69. The Court notes that the focus of the parties' arguments differed as regards the applicant company's role in the present case. The applicant company's argument was of the opinion that the applicant company was to be considered the discloser of the defamatory comments, whereas the applicant company considered that the comments had been published by third parties and the applicant company's freedom to impart information had been interfered with (see paragraphs 48 and 49 above). Regardless of whether the exact role to be attributed to the applicant company's activities, it is not, in substance, in dispute between the parties that the domestic courts' decisions in respect of the applicant company constituted an interference with its freedom of expression guaranteed under Article 10 of the Convention.

The Court sees no reason to hold otherwise (see also paragraph 50 above).

70. Such an interference with the applicant company's right to freedom of expression must be "prescribed by law", have one or more legitimate aims in the light of paragraph 2 of Article 10, and be "necessary in a democratic society".

(b) Lawfulness
71. The Court reiterates that a norm cannot be regarded as a "law" within the meaning of Article 10 § 2 unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty. Whilst certainty is desirable, it may bring in its train excessive rigidity, and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague, and whose interpretation and application are questions of practice (see, for example, Lindon, Otchakovsky-Laurens and July v. France [GC], nos. 21279/02 and 3644/02, § 41, ECHR 2007-IV).

72. The Court further reiterates that the scope of the notion of foreseeability depends on a considerable degree on the content of the text in issue, the field it is designed to cover, and the number and status of those to whom it is addressed. A law may still satisfy the requirement of foreseeability even if the person concerned has to take appropriate legal advice to access, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. This is particularly true in relation to persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation. They can on this account be expected to take special care in assessing the risks that such activity entails (see Lindon, Otchakovsky-Laurens and July, loc. cit., with further references to Cantoni v. France, 15 November 1996, § 35, Reports of Judgments and Decisions 1996-V, and Chauvy and Others v. France, no. 64915/01, §§ 43-45, ECHR 2004-VI).

73. The Court notes that in the present case the parties' opinions differed as to the question whether the interference with the applicant company's freedom of expression was "prescribed by law". The applicant company argued that the domestic law did not entail a positive obligation to premonitor content posted by third persons, and that its liability was limited under the EU Directive on Electronic Commerce. The Government referred to the pertinent provisions of the civil law and domestic case-law, under which media publications were liable for their publications along with the authors.

74. As regards the applicant company's argument that its liability was limited under the EU Directive on Electronic Commerce and the Information Society Services Act, the Court notes that the domestic courts found that the applicant company's activities did not fall within the scope of these acts. The Court reiterates in this context that it is not its task to take the place of the domestic courts. It is primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation. The Court's role is confined to ascertaining whether the effects of such an interpretation are compatible with the Convention (see, among others, Pérez de Rada Cavanilles v. Spain, 28 October 1998, § 43, Reports of Judgments and Decisions 1998-VIII).

75. The Court further notes that pursuant to the pertinent provisions of the Constitution, the Civil Code (General Principles) Act and the Obligations Act (see paragraphs 31 to 36 above), as interpreted and applied by the domestic courts, the applicant company was deemed liable for the publication of the defamatory comments. Although these provisions are quite general and lack detail in comparison with, for example, the Information Society Services Act (see paragraph 37 above), the Court is satisfied that they, along with the pertinent case-law, made it clear that a media publisher was liable for any defamatory statements made in its media publication. The fact that in the present case publication of articles and comments on an Internet portal was also found to amount to journalistic activity and the administrator of the portal as an entrepreneur was deemed to be a publisher can be seen, in the Court's view, as application of the existing tort law to a novel area related to new technologies (compare, for example, Bernh Larsen Holding AS and Others v. Norway, no. 24117/08, § 126, 14 March 2013, where the Court saw no reason to question the domestic court's interpretation, according to which legal provisions originally conceived in respect of hard copies of documents were also deemed to apply to electronic media documents). This does not mean that the provisions of the civil law in question did not constitute a sufficiently clear legal basis for the applicant company's liability, or that gradual clarification of legal rules was outlawed (compare, mutatis mutandis, Radio France and Others v. France, no. 539/04/00, §§ 20 and 30, ECHR 2004-IV).

Indeed, general provisions of law can at times make for a better adaptation to changing circumstances than can attempts at detailed regulation (see, for comparison, Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2) nos. 3002/03 and 23676/03, §§ 20, 21 and 38, ECHR 2009, where the "Internet publication rule" relied on a rule originally dating from the year 1849, and Editorial Board of Prawoje Delo and Shtekel v. Ukraine, no. 33014/05, §§ 60-68, ECHR 2011 (extracts), where the lack of reference to Internet publications in the otherwise quite detailed media law gave rise to an issue of lawfulness under Article 10 of the Convention).

76. The Court accordingly finds that, as a professional publisher, the applicant company must at least have been familiar with the legislation and case-law, and could also have sought legal advice. The Court observes in this context that the Delfi news portal is one of the largest in Estonia, and also that a degree of notoriety has been attributable to comments...
posted in its commenting area. Thus, the Court considers that the applicant company was in a position to assess the risks related to its activities and that it must have been able to foresee, to a reasonable degree, the consequences which these could entail. It therefore finds that the interference in issue was "prescribed by law", within the meaning of the second paragraph of Article 10 of the Convention.

(c) Legitimate aim

77. The Court considers that the restriction of the applicant company's freedom of expression pursued a legitimate aim of protecting the reputation and rights of others. The Court has taken note of the applicant company's argument about the liability of the actual authors of the comments. However, in the Court's view the fact that the actual authors were also in principle liable does not remove the legitimate aim of holding the applicant company liable for any damage to the reputation and rights of others. The question of whether the applicant company's rights under Article 10 were excessively restricted in the present case by holding it liable for comments written by third parties is a question of whether the restriction was "necessary in a democratic society", to be dealt with below.

(d) Necessary in a democratic society

(i) General principles

78. The fundamental principles concerning the question whether an interference with freedom of expression is "necessary in a democratic society" are well established in the Court's case-law and have been summarised as follows (see, among other authorities, Hertel v. Switzerland, 25 August 1998, § 46, Reports of Judgments and Decisions 1998–VI; Steel and Morris v. the United Kingdom, no. 68416/01, § 87, ECHR 2005–II; Mouvement raïlien suisse v. Switzerland [GC], no. 16354/06, § 48, ECHR 2012 (extracts)); and Animal Defenders International v. the United Kingdom [GC], no. 48876/08, § 100, 22 April 2013:

"(i) Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment. Subject to paragraph 2 of Article 10, it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no "democratic society". As set forth in Article 10, this freedom is subject to exceptions, which... must, however, be construed strictly, and the need for any restrictions must be established convincingly...

(ii) The adjective 'necessary', within the meaning of Article 10 § 2, implies the existence of a "pressing social need". The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court. The Court is therefore empowered to give the final ruling on whether a restriction is reconcilable with freedom of expression as protected by Article 10.

(iii) The Court's task, in exercising its supervisory jurisdiction, is not to take the place of the competent national authorities but rather to review under Article 10 the decisions they delivered pursuant to their power of appreciation. This does not mean that the supervision is limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith; what the Court has to do is to look at the interference complained of in the light of the case as a whole and determine whether it was 'proportionate to the legitimate aim pursued' and whether the reasons adduced by the national authorities to justify it are 'relevant and sufficient'... In doing so, the Court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 10 and, moreover, that they relied on an acceptable assessment of the relevant facts..."
84. Turning to the present case, the Court notes at the outset that there is no dispute that comments posted by readers in reaction to the news article published on the applicant company’s Internet news portal were of defamatory nature. Indeed, the applicant company promptly removed the comments once it was notified by the injured party, and described them as “infringing” and “illicit” before the Court. However, the parties’ views differ as to whether the applicant company was liable for the comments, and whether they amounted to a disproportionate interference with its freedom of expression. In other words, the question is whether the applicant company’s obligation, as established by the domestic judicial authorities, to ensure that comments posted on its Internet portal did not infringe the personality rights of third persons was in accordance with the guarantees set out in Article 10 of the Convention.

85. In order to resolve this question, the Court will proceed to analyse in turn a number of factors which it considers to be of importance in the circumstances of the present case. Firstly, the Court will examine the context of the comments, secondly, the measures applied by the applicant company in order to prevent or remove defamatory comments, thirdly, the liability of the actual authors of the comments as an alternative to the applicant company’s liability, and fourthly the consequences of the domestic proceedings for the applicant company.

86. The Court notes that the notice published on the Delfi news portal addressed a topic of a certain degree of public interest. It discussed a shipping company’s moving its ferries from one route to another and in doing so breaking the ice at potential locations of ice roads, as a result of which the opening of such roads – a cheaper and faster connection to the islands compared to the company’s ferry services – was postponed for several weeks. The article itself was a balanced one, a manager of the shipping company was given the opportunity to provide explanations, and the article contained no offensive language. Indeed, the article itself gave rise to no arguments about defamation in the domestic proceedings. Nevertheless, the article dealt with the shipping company’s activities that negatively affected a large number of people. Therefore, the Court considers that the applicant company, by publishing the article in question, could have realised that it might cause negative reactions against the shipping company and its managers and that, considering the general reputation of comments on the Delfi news portal, there was a higher-than-average risk that the negative comments could go beyond the boundaries of acceptable criticism and reach the level of gratuitous insult or hate speech. It also appears that the number of comments posted on the article in question was abnormal, and that information contained in them indicated a wide audience for the comments. The Court concludes that the applicant company was expected to exercise a degree of caution in the circumstances of the present case in order to avoid being held liable for an infringement of others’ reputations.

87. As regards the measures applied by the applicant company, the Court notes that, in addition to the disclaimer stating that the writers of the comments – and not the applicant company – were accountable for them, and that it was prohibited to post comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, the applicant company had two general mechanisms in operation. Firstly, it had an automatic system of deletion of comments based on stems of certain vulgar words. Secondly, it had a notice-and-take-down system in place according to which anyone could n...

88. The Court has further had regard to the notice-and-take-down system as used by the applicant company. Indeed, the question of whether by applying this system the applicant company had fulfilled its obligation of diligence was one of the main points of disagreement between the parties in the present case. The Court firstly notes that the technical solution related to the Delfi portal’s notice-and-take-down system was easily accessible and convenient for users – there was no need to take any steps other than clicking on a button provided for that purpose. There was no need to formulate reasons as to why a comment was considered inappropriate or to send a letter to the applicant company with the pertinent request. Although in the present case the interested person did not use the notice-and-take-down feature offered by the applicant company on its website, but rather relied on making a claim in writing and sending it by mail, this was his own choice, and in any event there is no dispute that the defamatory comments were removed by the applicant company without delay after receipt of the notice. Nevertheless, by that time the comments had already been accessible to the public for six weeks.

89. The Court notes that the interested person’s opinion, shared by the domestic courts, the prior automatic filtering and notice-and-take-down system used by the applicant company did not ensure sufficient protection for the rights of third persons. The domestic courts attached importance in this context to the fact that the publication of the news articles and making public the readers’ comments on these articles was part of the applicant company’s professional activity. It was interested in the number of readers as well as comments, on which its advertising revenue depended. The Court considers this argument pertinent in determining the proportionality of the interference with the applicant company’s freedom of expression. It also finds that publishing defamatory comments on a large Internet news portal, as in the present case, implies a wide audience for the comments. The Court further notes that the applicant company – and not a person whose reputation could be at stake – was in a position to know about an article to be published or to predict the nature of the possible comments prompted by it and, above all, to take technical or manual measures to prevent defamatory statements from being made public. Indeed, the actual writers of comments could not modify or delete their comments once posted on the Delfi news portal – only the applicant company had a technical means of interest in the matter among the readers and those who posted their comments. Thus, the Court concludes that the applicant company had fulfilled its duty of diligence was one of the main points of disagreement between the parties in the present case. The Court firstly notes that the technical solution related to the Delfi portal’s notice-and-take-down system was easily accessible and convenient for users – there was no need to take any steps other than clicking on a button provided for that purpose. There was no need to formulate reasons as to why a comment was considered inappropriate or to send a letter to the applicant company with the pertinent request. Although in the present case the interested person did not use the notice-and-take-down feature offered by the applicant company on its website, but rather relied on making a claim in writing and sending it by mail, this was his own choice, and in any event there is no dispute that the defamatory comments were removed by the applicant company without delay after receipt of the notice. Nevertheless, by that time the comments had already been accessible to the public for six weeks.

90. The Court has also had regard to the fact that the domestic courts did not make any orders to the applicant company as to how the latter should ensure the protection of third parties’ rights, leaving the choice to the applicant company. Thus, no specific measures such as a requirement of prior registration of users before they were allowed to post comments, monitoring comments, imposing the applicant company’s obligation to remove comments before making them public, or speedy review of comments after posting, to name just a few, were imposed on the applicant company. The Court considers the leeway left to the applicant company in this respect to be an important factor reducing the severity of the interference with its freedom of expression.

91. The Court has taken note of the applicant company’s argument that the affected person could have brought a claim against the actual authors of the comments. It attaches more weight, however, to the Government’s counter-argument that for the purposes of bringing a civil claim it was very difficult for an individual to establish the identity of the persons to be sued. Indeed, for purely technical reasons it would appear...
disproportionate to put the onus of identification of the authors of defamatory comments on the injured person in a case like the present one. Keeping in mind the State’s positive obligations under Article 8 that may involve the adoption of measures designed to secure respect for private life in the sphere of the relations of individuals between themselves (see Von Hannover (no. 2), cited above, § 98, with further references), the Court is not convinced that measures allowing an injured party to bring a claim only against the authors of defamatory comments – as the applicant company appears to suggest – would have, in the present case, guaranteed effective protection of the injured person’s right to private life. It notes that it was the applicant company’s choice to allow comments by non-registered users, and that by doing so it must be considered to have assumed a certain responsibility for these comments.

92. The Court is mindful, in this context, of the importance of the wishes of Internet users not to disclose their identity in exercising their freedom of expression. At the same time, the spread of the Internet and the possibility – or for some purposes the danger – that information once made public will remain public and circulate forever, calls for caution. The ease of disclosure of information on the Internet and the substantial amount of information there means that it is a difficult task to detect defamatory statements and remove them. This is so for an Internet news portal operator, as in the present case, but this is an even more onerous task for a potentially injured person, who would be less likely to possess the resources for continual monitoring of the Internet. The Court considers the latter element an important factor in balancing the rights and interests at stake. It also refers, in this context, to the Krone Verlag (no. 4) judgment, where it found that shifting the defamed person’s risk to obtain redress for defamation proceedings to the media company, usually in a better financial position than the defamer, was not as such a disproportionate interference with the media company’s right to freedom of expression (see Krone Verlag GmbH & Co. KG v. Austria (no. 4), no. 72331/01, § 32, 9 November 2006).

93. Lastly, the Court notes that the applicant company was obliged to pay the affected person the equivalent of EUR 320 in non-pecuniary damages. The Court is of the opinion that this sum, also taking into account that the applicant company was a professional operator of one of the largest Internet news portals in Estonia, can by no means be considered disproportionate to the breach established by the domestic courts.

94. Based on the above elements, in particular the insulting and threatening nature of the comments, the fact that the comments were posted in reaction to an article published by the applicant company in its professionally-managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to avoid damage being caused to other parties’ reputations and to ensure a realistic possibility that the authors of the comments will be held liable, and the moderate sanction imposed on the applicant company, the Court considers that in the present case the domestic courts’ finding that the applicant company was liable for the defamatory comments posted by readers on its Internet news portal was a justified and proportionate restriction on the applicant company’s right to freedom of expression.

There has accordingly been no violation of Article 10 of the Convention.

FOR THESE REASONS, THE COURT UNANIMOUSLY
1. Declares the application admissible;
2. Holds that there has been no violation of Article 10 of the Convention.
VI. Cybercrime and Cybersecurity

Convention on Cybercrime

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;


Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;
Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1.a.i of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data,
b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

title 3 – content-related offences

article 9 – offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;
b offering or making available child pornography through a computer system;
c distributing or transmitting child pornography through a computer system;
d procuring child pornography through a computer system for oneself or for another person;
e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;
b a person appearing to be a minor engaged in sexually explicit conduct;
c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;
b an authority to take decisions on behalf of the legal person;
c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are...
punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditions preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditions preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and
b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
CASEBOOK OF ICT LAW
2015

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1b through 1d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denotate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requesting Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that rendered impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly
transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a. the authority seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information identifying the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the
Chapter IV – Final provisions

Article 37 – Accession to the Convention

1. After the entry into force of the Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the declaration.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

   a. the provision of technical advice;

   b. the preservation of data pursuant to Articles 29 and 30;

   c. the collection of evidence, the provision of legal information, and locating of suspects.

2. A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

The Parties shall provide mutual assistance to each other in the real-time collection of traffic data.

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;

b. the preservation of data pursuant to Articles 29 and 30;

c. the collection of evidence, the provision of legal information, and locating of suspects.

In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the declaration.

This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the declaration.
the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention’s objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibilities of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement...
of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention’s provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretory General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms
and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as “the Convention”), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

"racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

1 Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) distributing, or otherwise making available, racist and xenophobic material to the public through a computer system;

2 A Party may reserve the right not to apply, in whole or in part, paragraph 1 to expose hatred, contempt or ridicule;

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 4 – Racist and xenophobic motivated threat

1 Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

(a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule;

(b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

(a) distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either:

(a) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

(b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish such criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, mutatis mutandis, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Article IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

(a) signature without reservation as to ratification, acceptance or approval;

(b) subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States have expressed their
I. The Convention and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001) and the Convention has been opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cyber-crime.

II. The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein.

I. Introduction
1. The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.
2. A conspicuous feature of information technology is the impact it has had and will have on the evolution of telecommunications technology. Classical telephony, involving the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. Circuit-switched connections have been replaced by packet-switched networks. It is no longer relevant whether a direct connection can be established; it suffices that data is entered
into a network with a destination address or made available for anyone who wants to access it.

3. The pervasive use of electronic mail and the accessing through the Internet of numerous web sites are examples of these developments. They have changed our society profoundly.

4. The ease of accessibility and searchability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has lead to an explosive growth in the amount of information available and the knowledge that can be drawn therefrom.

5. These developments have given rise to an unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be far-reaching more than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality.

Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour.

6. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge in the amount of information available and the knowledge that can be drawn therefrom.

7. By decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. The CDPC based its decision on the following considerations:

8. "The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.

9. The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Whilst Recommendation No. (89) 9 resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as measures that are closely connected with the use of information technology, should be addressed."

10. In addition, the CDPC took into account the Report, prepared – at its request – by Professor H.W.K. Kaspersen, which concluded that "... it should be looked to another legal instrument with more engagement than a Recommendation, such as a Convention. Such a Convention should not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements." (1) A similar conclusion emerged already from the Report attached to Recommendation N° R (89) 9 (2) concerning substantive law and from Recommendation N° R (95) 13 (3) concerning problems of procedural law connected with information technology.

11. The new committee's specific terms of reference were as follows:

i. "Examine, in the light of Recommendations N° R (89) 9 on computer-related crime and No R (95) 13 concerning problems of criminal procedural law connected with information technology, in particular the following subjects:

ii. cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;

iii. other substantive criminal law issues where a common approach may be of the purpose of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;

iv. the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption;

v. the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti) and which law should accordingly apply, including the problem of his identity in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;

vi. questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).

The Committee should draft a binding legal instrument, as far as possible, on the items i) – vi), with particular emphasis on international questions and, if appropriate, accessory recommendations regarding specific issues. The Committee may make suggestions on other issues in the light of technological developments."

12. Further to the CDPC's decision, the Committee of Ministers set up the new committee, called "the Committee of Experts on Crime in Cyber-space (PC-CY)" by decision n° CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers' Deputies (held on 4 February 1997). The Committee PC-CY started its work in April 1997 and undertook negotiations on a draft international convention on cyber-crime. Under its original terms of reference, the Committee was due to finish its work by 31 December 1999. Since by that time the Committee was not yet in a position to fully conclude its negotiations on certain issues in the draft Convention, its terms of reference were extended by decision n° CM/Del/Dec(99)679 of the Ministers' Deputies until 31 December 2000. The European Ministers of Justice expressed their support twice concerning the negotiations: by Resolution No. 1, adopted at their 21st Conference (Prague, June 1997).
which recommended the Committee of Ministers to support the work carried out by the CDPC on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as by Resolution No 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cyber-crime. The member States of the European Union expressed their support to the work of the PC-CY through a Joint Position, adopted in May 2000.

13. Between April 1997 and December 2000, the Committee PC-CY held 10 meetings in plenary and 15 meetings of its open-ended Drafting Group. Following the expiry of its extended terms of reference, the experts held, under the aegis of the CDPC, three more meetings to finalise the draft Explanatory Memorandum and review the draft Convention in the light of the opinion of the Parliamentary Assembly. The Assembly was requested by the Committee of Ministers in October 2000 to give an opinion on the draft Convention, which it adopted at the 2nd part of its plenary session in April 2001.

14. Following a decision taken by the Committee PC-CY, an early version of the draft Convention was declassified and released in April 2000, followed by subsequent drafts released after each plenary meeting, in order to enable the negotiating States to consult with all interested parties. This consultation process proved useful.

15. The revised and finalised draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature.

III. The Convention

16. The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.

17. The Convention, accordingly, contains four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation; (IV) Final clauses.

18. Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

19. Section 2 of Chapter II (procedural law issues) – the scope of which goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form – determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. It then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data. Chapter II ends with the jurisdiction provisions.

20. Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.

21. Finally, Chapter IV consists the final clauses, which – with certain exceptions – repeat the standard provisions in Council of Europe treaties.

Commentary on the articles of the Convention

Chapter I – Use of terms

Introduction to the definitions at Article 1

22. It was understood by the drafters that under this Convention Parties would not be obliged to copy verbatim into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation.

Article 1 (a) – Computer system

23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices called "Automatic" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

Article 1 (b) – Computer data

25. The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion " computer data " is introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

Article 1 (c) – Service provider

26. The term "service provider" encompasses a broad category of persons that play a particular role with regard to
communication or processing of data on computer systems (cf. also comments on Section 2). Under (j) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

27. Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (j). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (j). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his website) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.

Article 1 (g) – Traffic data

28. For the purposes of this Convention traffic data as defined in article 1, under subparagraph d, is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route communication from its origin to its destination. It is therefore auxiliary to the communication itself.

29. In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collating further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication’s route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn’t reveal the content of the communication which is regarded to be more sensitive.

30. The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

31. The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. In this context, Article 15 obliges the Parties to provide for conditions and safeguards that are adequate for protection of human rights and liberties. This implies, inter alia, that the substantive criteria and the procedure to apply an investigative power may vary according to the sensitivity of the data.

Chapter II – Measures to be taken at the national level

32. Chapter II (Articles 2 – 22) contains three sections: substantive criminal law (Articles 2 – 13), procedural law (Articles 14 – 21) and jurisdiction (Article 22).

Section I – Substantive criminal law

33. The purpose of Section I of the Convention (Articles 2 – 13) is to improve the means to prevent and suppress computer- or computer- related crime by establishing a common minimum standard of relevant offences. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too. International co-operation (esp. extradition and mutual legal assistance) is facilitated e.g. regarding requirements of double criminality.

34. The list of offences included represents a minimum consensus not excluding extensions in domestic law. To a great extent it is based on the guidelines developed in connection with Recommendation No. R (89) 9 of the Council of Europe on computer-related crime and on the work of other public and private international organisations (OECD, UN, AIDP), but taking into account more modern experiences with abuses of expanding telecommunication networks.

35. The section is divided into five titles. Title I includes the core of computer-related offences, offences against the confidentiality, integrity and availability of computer data and systems, representing the basic threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed. The heading describes the type of crimes which are covered, that is the unauthorised access to and illicit tampering with systems, programmes or data, and the destruction of data. Title II covers the ‘computer-related offences’, which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected already by criminal law against attacks using traditional means. The Title II offences (computer-related fraud and forgery) have been added by following suggestions in the guidelines of the Council of Europe Recommendation No. R (89) 9. Title III covers the ‘content-related offences of unlawful production or distribution of child pornography by use of computer systems as one of the most dangerous modi operandi in recent times. The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the present Convention.

Title IV sets out ‘offences related to infringements of copyright and related rights’. This was included in the Convention because copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern. Finally, Title V includes additional provisions on attempt, aiding and abetting and sanctions and measures, and, in compliance with recent international instruments, on corporate liability.

36. Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.

37. The drafters of the Convention understood that Parties may exclude petty or insignificant misconduct from implementation of the offences defined in Articles 2-10. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The
expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's governmental acts to maintain public order and safety, to prevent crime (including the enforcement of national security or investigation of criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

39. All the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. For instance, in Article 8 on computer-related fraud, the intent to procure an economic benefit is a constituent element of the offence. The drafters of the Convention agreed that the exact meaning of 'intentionally' should be left to national interpretation.

40. Certain articles in the section allow the addition of qualifying circumstances when implementing the Convention in their national law. In other instances even the possibility of a reservation is granted (cf. Articles 40 and 42). These different ways of a more restrictive approach in criminalisation reflect different assessments of the dangerousness of the behaviour involved or of the need to use criminal law as a countermeasure. This approach provides flexibility to governments and parliaments in determining their criminal policy in this area.

41. Laws establishing these offences should be drafted with as much clarity and specificity as possible, in order to provide adequate foreseeability of the type of conduct that will result in a criminal sanction.

42. In the course of the drafting process, the drafters considered the advisability of criminalising conduct other than those defined at Articles 2 – 41, including the so-called cyber-squatting, i.e. the fact of registering a domain-name which is identical either to the name of an entity that already exists and is usually well-known or to the trade-name or trademark of a product or company. Cyber-squatters have no intent to make an active use of the domain-name and seek to obtain a financial advantage by forcing the entity concerned, even though indirectly, to pay for the transfer of the ownership over the domain-name. At present this conduct is considered as a trademark-related issue. As trademark violations are not governed by this Convention, the drafters did not consider it appropriate to deal with the issue of criminalisation of such conduct.

Title I – Offences against the confidentiality, integrity and availability of computer data and systems

43. The criminal offences defined under (Articles 2–6) are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

Illegal access (Article 2)

44. "Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.

46. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

47. The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of "cookies" or 'bots' to locate and retrieve information on behalf of communication. The application of such tools per se is not "without right". The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself "without right", in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of "cookies" by not rejecting the initial advantage used and giving consent.

49. Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the ECDC Working Party in 1985.

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked systems (under criminal law or otherwise).
computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extrarsets).

Illegal interception (Article 3)

51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

52. The text of the provision has been mainly taken from the offence of 'unauthorised interception' contained in Recommendation (89) 9. In the present Convention it has been made clear that the communications involved concern "transmissions of computer data" as well as electromagnetic radiation, under the circumstances as explained below.

53. Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software like passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

54. The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term 'non-public' does not per se exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR judgement in Halford v. UK case, 25 June 1997, 206/05/92).

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may regard as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of 'computer system' may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though 'non-public', takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

57. The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from the computer system is included as an offence under this provision.

58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing "cookies", is not intended to be criminalised as such, as not being an interception "without right". With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken "with right".

59. In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as "intentionally" and "without right".

Data interference (Article 4)

60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

61. In paragraph 1, 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deleted' data is an example of data in the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

62. The above acts are only punishable if committed "without right". Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g. software permitting access to the Internet that disables similar programs), and even if done unintentionally, and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (e.g. the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator or to commit criminal activity.

63. In addition, the offender must have acted "intentionally".

64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

System interference (Article 5)

65. This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems
including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.

66. The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data. 67. The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data with a particular system in a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

68. The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial activities are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such hindering must furthermore be "serious" in order to give rise to criminal sanction, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct is not criminalised by this article, even if it causes serious hindering.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries.

A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. "Distribution" refers to the active act of forwarding data to others, while "making available" refers to the placing online devices for the use of others. This term also intends to cover the creation of hyperlinks in order to facilitate access to such devices. The inclusion of a "computer programme" refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

73. The drafters debating whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of moral law has not been applied. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted, by the last phrase of paragraph 1(b), to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

76. The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e., direct) intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ("cracking-devices") and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be with right.

78. Due to different assessments of the need to apply the offence of "Misuse of Devices" to all of the different kinds of computer offences in Articles 2 – 5, paragraph 3 allows, on the basis of a reservation (cf. Article 42), to restrict the offence in domestic law. Each Party is, however, obliged to criminalise at least the sale, distribution or making available of a computer password or access data as described in paragraph 1(a) 2.

Title 2 – Computer-related offences

79. Articles 7 – 10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to
situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones.

80. "Computer-related forgery" and "Computer-related fraud" deal with certain computer-related offences, i.e. computer-related forgery and computer-related fraud as two specific kinds of manipulation of computer systems or computer data. Their inclusion acknowledges the fact that in many countries certain traditional legal interests are not sufficiently protected against new forms of interference and attacks.

Computer-related forgery (Article 7)

81. The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information. Data is manipulated in the data pool, i.e. the "deception" or "manipulation" is independent of a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

82. It should be noted that national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data.

83. This provision covers data which is the equivalent of a public or private document, which has legal effects. The unauthorised "input" of correct or incorrect data brings about a situation that corresponds to the making of a false document. Manipulations include alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document.

84. The term "for legal purposes" refers also to legal translation of documents which are legally relevant.

85. The final sentence of the provision allows Parties, when implementing the offence in domestic law, to require in addition an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer-related fraud (Article 8)

86. With the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.

87. To ensure that all possible relevant manipulations are covered, the constituent elements of "input", "alteration", "deletion" or "suppression" in Article 8(a) are supplemented by the general act of "interference with the functioning of a computer programme or system" in Article 8(b). The elements of "input, alteration, deletion or suppression" have the same meaning as in the previous articles. Article 8(b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

88. The computer fraud manipulations are criminalised if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term 'loss of property', being a broad notion, includes loss of money, tangibles and intangibles with an economic value.

89. The offence must be committed "without right", and the economic benefit must be obtained without right. Of course, legitimate common commercial practices, which are intended to procure an economic benefit, are not meant to be included in the offences established by this article because they are conducted with right. For example, activities carried out pursuant to a valid contract between the affected persons are with right (e.g. disabling a web site as entitled pursuant to the terms of the contract).

90. The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet ("bots"), even if not authorised by a site visited by the "bot" is not intended to be criminalised.

91. Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.

92. This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 – 11 October 1997) in their Action Plan (item II.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM(2000) 854).

93. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.

94. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system. This provision was felt necessary to combat the dangers described above at their source.

95. Paragraph 1(b) criminalises the 'offering' of child pornography through a computer system. 'Offering' is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. 'Making available' is intended to cover the placing of child pornography on line for the use of others.
e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography.

96. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system. ‘Distribution’ is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of ‘transmitting’ child pornography.

97. The term procuring for oneself or for another in paragraph 1(d) means actively obtaining child pornography, e.g. by downloading it.

98. The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.

99. The term ‘pornographic material’ in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which can be achieved by means of conversion into a visual image.

100. A ‘sexually explicit conduct’ covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

101. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although ‘realistic’, do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.

102. In the three cases covered by paragraph 2, the protected legal interests are slightly different. Paragraph 2(a) focuses more directly on the protection against child abuse. Paragraphs 2(b) and 2(c) aim at providing protection against behaviour which is not necessarily creating harm to the ‘child’ depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.

103. The term ‘without right’ does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, the term ‘without right’ allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a Party may provide a defence in respect of conduct related to “pornographic material” having an artistic, medical, scientific or similar merit. In relation to paragraph 2(b), the reference to ‘without right’ could also allow, for example, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a minor in the sense of this provision.

104. Paragraph 3 defines the term ‘minor’ in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a ‘child’ in the UN Convention on the Rights of the Child (Article 1). It was considered an important policy matter to set a uniform international standard regarding age. It should be noted that the age refers to the use of (real or fictitious) children as sexual objects, and is separate from the age of consent for sexual relations.

Nevertheless, recognising that certain States require a lower age-limit in national legislation regarding child pornography, the last phrase of paragraph 3 allows Parties to require a different age-limit, provided it is not less than 16 years.

105. This article lists different types of illicit acts related to child pornography which, as in articles 2 – 8, Parties are obligated to criminalise if committed “intentionally.” Under this standard, a person is not liable unless he has an intent to offer, make available, distribute, transmit, produce or possess child pornography. Parties may adopt a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is “knowledge and control” over the information which is transmitted or stored. It is not sufficient, for example, that a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

106. Paragraph 4 permits Parties to make reservations regarding paragraph 1(d) and (e), and paragraph 2(b) and (c). The right not to apply these sections of the provision may be made in part or in whole. Any such reservation should be declared to the Secretary General of the Council of Europe at the time of signature or ratification or when depositing the Party’s instruments of ratification, acceptance, approval or accession, in accordance with Article 42.

Title 4 – Offences related to infringements of copyright and related rights

107. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audio-visual and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international co-operation in this field.

108. Each Party is obliged to criminalise willful infringements of copyright and related rights, sometimes referred to as neighbouring rights, that the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale”. Paragraph 1 provides for criminal sanctions against infringements of copyright by means of a computer system. Infringement of copyright is already an offence in almost all States. Paragraph 2 deals with the infringement of related rights by means of a computer system.

109. Infringement of both copyright and related rights is as defined under the law of each Party and pursuant to the obligations the Party has undertaken in respect of certain international instruments. While each Party is required to establish as criminal offences those infringements, the precise manner in which such infringements are defined under domestic law may vary from State to State. However, criminalisation obligations under the Convention do not cover intellectual property infringements other than those explicitly addressed in Article 10 and thus exclude patent or trademark-related violations.

110. With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation
Performances and Phonograms Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply the agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.

111. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty had not entered into force at the time of concluding the present Convention. These treaties are nevertheless important as they significantly update the international protection for intellectual property (especially with regard to the new right of 'making available' of protected material 'on demand' over the Internet) and improve the means to fight violations of intellectual property rights worldwide. However it is understood that the infringements of rights established by these treaties need not be criminalised under the present Convention until these treaties have entered into force with respect to a Party.

112. The obligation to criminalise infringements of copyright and related rights pursuant to obligations undertaken in international instruments does not extend to any moral rights conferred by the named instruments (such as in Article 6bis of the Bern Convention and in Article 5 of the WIPO Copyright Treaty).

113. Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations.

114. The provisions are intended to provide for criminal sanctions against infringements 'on a commercial scale' and by means of a computer system. This is in line with Article 61 of the TRIPS Agreement which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale". However, Parties may wish to go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.

115. The term "without right" has been omitted from the text of this article as redundant, since the term "infringement" already denotes use of the copyrighted material without authorisation. The absence of the term "without right" does not contra prohibere application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

116. Paragraph 3 allows Parties not to impose criminal liability under paragraphs 1 and 2 in "limited circumstances" (e.g. parallel imports, rental rights), as long as other effective remedies, including civil and/or administrative measures, are available. This provision essentially allows Parties a limited exemption from the obligation to impose criminal liability, provided that they do not derogate from obligations under Article 61 of the TRIPS Agreement, which is the minimum pre-existing criminalisation requirement.

117. This article shall in no way be interpreted to extend the protection granted to authors, film producers, performers, producers of phonograms, broadcasting organisations or other right holders to persons that do not meet the criteria for eligibility under domestic law or international agreement.

Title 5 – Ancillary liability and sanctions

Attempt and aiding or abetting (Article 11)

118. The purpose of this article is to establish additional offences related to attempt and aiding or abetting the commission of the offences defined in the Convention. As discussed further below, it is not required that a Party criminalise the attempt to commit each offence established in the Convention.

119. Paragraph 1 requires Parties to establish as criminal offences aiding or abetting the commission of any of the offences under Article 10. Liability arises for aiding or abetting where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. For example, although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

120. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt (for example, the elements of offering or making available of child pornography). Moreover, some legal systems limit the offences for which the attempt is punished. Accordingly, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c).

121. As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

122. Paragraph 3 was added to address the difficulties Parties may have with paragraph 2, given the widely varying concepts in different legislations and despite the effort in paragraph 2 to exempt certain aspects from the provision on attempt. A Party may declare that it reserves the right not to apply paragraph 2 in part or in whole. This means that any Party making a reservation as to that provision will have no obligation to criminalise attempt at all, or may select the offences or parts of offences to which it will attach criminal sanctions in relation to attempt. The reservation aims at enabling the widest possible ratification of the Convention while permitting Parties to preserve some of their fundamental legal concepts.

Corporate liability (Article 12)

123. Article 12 deals with the liability of legal persons. It is consistent with the current legal trend to recognise corporate liability. It is intended to impose liability on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the corporation. The term "without right" does not contra prohibere application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

124. Under paragraph 1, four conditions need to be met for liability to attach. First, one of the offences described in the Convention must have been committed. Second, the offence must have been committed for the benefit of the legal person. Third, a person who has a leading position must have committed the offence (including aiding and abetting). The term "person who has a leading position" refers to a natural person who has a high position in the organisation, such as a director. Fourth, the person who has a leading position must have acted on the basis of one of these powers – a power of representation or an authority to take decisions or to exercise control – which demonstrate that such a physical person acted within the scope of his or her authority to engage the liability of the legal person. In sum, paragraph 1 obligates Parties to have the ability to impose liability on the legal person only for offences committed by such leading persons.

125. In addition, Paragraph 2 obligates Parties to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person's authority, i.e., one of its employees or agents acting
within the scope of their authority. The conditions that must be fulfilled before liability can attach are that (1) an offence has been committed by such an employee or agent of the legal person, (2) the offence has been committed for the benefit of the legal person; and (3) the commission of the offence has been made possible by the leading person having failed to supervise the employee or agent. In this context, failure to supervise should be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person. Such appropriate and reasonable measures could be determined by various factors, such as the type of the business, its size, the standards or the established business best practices, etc. This should not be interpreted as requiring a general surveillance regime over employee communications (see also paragraph 54). A service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person, because the term “acting under its authority” applies exclusively to employees and agents acting within the scope of their authority.

126. Liability under this Article may be criminal, civil or administrative. Each Party has the flexibility to choose to provide for any or all of these forms of liability, in accordance with the legal principles of each Party, as long as it meets the criteria of Article 13, paragraph 2, that the sanction or measure be “effective, proportionate and dissuasive” and includes monetary sanctions.

127. Paragraph 4 clarifies that corporate liability does not exclude individual liability.

Sanctions and measures (Article 13)

128. This article is closely related to Articles 2-11, which define various computer- or computer-related crimes that should be made punishable under criminal law. In accordance with the obligations imposed by those articles, this provision obliges the Contracting Parties to draw consequences from the serious nature of these offences by providing for criminal sanctions that are ‘effective, proportionate and dissuasive’ and, in the case of natural persons, include the possibility of imposing prison sentences.

129. Legal persons whose liability is to be established in accordance with Article 12 shall also be subject to sanctions that are ‘effective, proportionate and dissuasive’, which can be criminal, administrative or civil in nature. Contracting Parties are compelled, under paragraph 2, to provide for the possibility of imposing monetary sanctions on legal persons.

130. The article leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences, for example, measures could include injunction or forfeiture. It leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems.

Section 2 – Procedural law

131. The articles in this Section describe certain procedural measures to be taken at the national level for the purpose of criminal investigation of the offences established in Section 1, other criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence. In accordance with Article 39, paragraph 3, nothing in the Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor precludes a Party from doing so.

132. The technological revolution, which encompasses the “electronic highway” where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers.

133. One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.

134. The Convention adapts traditional procedural measures, such as search and seizure, to the new technological environment. Additionally, new measures have been created, such as expedited preservation of data, in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment. As data in the new technological environment is not always static, but may be flowing in the process of communication, other traditional collection procedures relevant to telecommunications, such as real-time collection of traffic data and interception of content data, have also been adapted in order to permit the collection of electronic data that is in the process of communication. Some of these measures are set out in Council of Europe Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology.

135. All the provisions referred to in this Section aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings. The drafters of the present Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.

136. The procedures in general refer to all types of data, including three specific types of computer data (traffic data, content data and subscriber data), which may exist in two forms (stored or in the process of communication). Definitions of some of these terms are provided in Articles 1 and 18. The applicability of a procedure to a particular type or form of electronic data depends on the nature and form of the data and the nature of the procedure, as specifically described in each article.

137. In adapting traditional procedural laws to the new technological environment, the question of appropriate terminology arises in the provisions of this section. The options included maintaining traditional language (‘search’ and ‘seize’), using new and more technologically oriented computer terms (‘access’ and ‘copy’), as adopted in texts of other international fora on the subject (such as the G8 High Tech Crime Subgroup), or employing a compromise of mixed language (‘search or similarly access’, and ‘seize or similarly secure’). As there is a need to reflect the evolution of concepts in the electronic environment, as well as identify and maintain their traditional roots, the flexible approach of allowing States to use either the old notions of “search and seizure” or the new notions of “access and copying” is employed.

138. All the articles in the Section refer to “competent authorities” and the powers they shall be granted for the purposes of specific criminal investigations or proceedings. In certain countries, only judges have the power to order or authorise the collection or production of evidence, while in other countries prosecutors or other law enforcement officers are entrusted with the same or similar powers. Therefore, ‘competent authority’ refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Title 1 – Common provisions
139. The Section begins with two provisions of a general nature that apply to all the articles relating to procedural law. Scope of procedural provisions (Article 14)
140. Each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal framework, to establish the powers and procedures described in this Section for the purpose of "specific criminal investigations or proceedings."
141. Subject to two exceptions, each Party shall apply the powers and procedures established in accordance with this Section to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. Thus, for the purpose of specific criminal investigations or proceedings, the powers and procedures referred to in this Section shall be applied to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. This ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section. It ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data. The Convention makes it explicit that Parties should incorporate into their laws the possibility that information obtained and preserved in digital form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.
142. There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Many States limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure. Likewise, this Convention only requires Parties to establish interception powers and procedures in relation to content data of specified computer communications in respect of a range of serious offences to be determined by domestic law.
143. Second, a Party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in Article 21. Some States consider the collection of traffic data as being justified in the context of crime prevention and the collection of data in terms of privacy and intrusiveness. The right of reservation would permit these States to limit the application of the measures to collect traffic data, in real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data. Many States, however, do not consider the interception of content data and the collection of traffic data to be equivalent in terms of privacy interests and degree of intrusiveness, as the collection of traffic data alone does not collect or disclose the content of the communication. As the real-time collection of traffic data can be very important in tracking the source or destination of computer communications (thus, assisting in identifying criminals), the Convention invites Parties that exercise the right of reservation to limit their reservation so as to enable the broadest application of the powers and procedures provided to collect, in real-time, traffic data.
144. Paragraph (b) provides a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention's adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users and which do not use public communications networks nor are they connected with other computer systems. The term "closed group of users" refers, for example, to a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to communicate amongst themselves using a computer network. The term "not connected with other computer systems" means that, at the time an order under Articles 20 or 21 would be issued, the system on which communications are being transmitted does not have a physical or logical connection to another computer network. The term "does not employ public communications networks" excludes systems that use public computer networks (public telecommunication facilities or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users.

Conditions and safeguards (Article 15)
145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively or judicially, that the modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards that each Party may provide for in its domestic law and procedures. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005 (4), 009, 046, 114, 117 and 177), as well as other instruments that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.
146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislations. Thus, the protection that the powers and procedures shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.
147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other
independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation by national authorities of particular conditions and safeguards. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

140. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interest in freedom and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.

Title 2 - Expedited preservation of stored computer data

149. The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. They do not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications. These issues are addressed in Title 5.

150. The measures described in the articles operate only where computer data already exists and is currently being stored. For many reasons, computer data relevant for criminal investigations may not exist or no longer be stored. For example, some data may not have been collected and retained, or if collected was not maintained. Data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings. Sometimes there may be no business reason for the collection and retention of data, such as where customers have a contract and the respect for privacy is free. Article 16 and 17 do not address these problems.

151. "Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

152. Articles 16 and 17 refer only to data preservation, and not data retention. They do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. The preservation measures apply to computer data that "has been stored by means of a computer system", which presupposes that the data already exists, has already been collected and is stored. Furthermore, as indicated in Article 14, all of the powers and procedures required to be established in Section 2 of the Convention are "for the purpose of specific criminal investigations or proceedings", which limits the application of the measures to an investigation in a particular case. Additionally, where a Party gives effect to preservation measures by means of an order, this order is in relation to "specified stored computer data in the person's possession or control" (paragraph 2). The articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.

153. The obligation to ensure preservation of data is not intended to require Parties to restrict the offering or use of services that do not routinely collect and retain certain types of data, such as traffic or subscriber data, as part of their legitimate business practices. Neither does it require them to implement new technical safeguards to do so, e.g., to preserve ephemeral data, which may be present on the system for such a brief period that it could not be reasonably preserved in response to a request or an order.

154. Some States have laws that require that certain types of data, such as personal data, held by particular types of holders must not be retained and must be deleted if there is no longer a business purpose for the retention of the data. In the European Union, the general principle is implemented by Directive 95/46/EC and, in the particular context of the telecommunications sector, Directive 97/66/EC. These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. These directives do not prevent member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specific investigations.

155. Data preservation is for most countries an entirely new legal power or procedure in domestic law. It is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. First, because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. However, where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data. For legitimate business practices, a preservation order may also be less disruptive to its normal activities and reputation than the execution of a search and seizure of its premises. Second, computer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. These communications may contain illegal content, such as child pornography, computer viruses or other instructions that cause interference with data or the proper functioning of the computer system, or evidence of the commission of other crimes, such as drug trafficking or fraud. Determining the source, destination or route of such communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required (see further explanation on the importance of traffic data below under Article 17). Third, where these communications contain illegal content or evidence of criminal activity and copies of such communications are retained by service providers, such as e-mail, the preservation of these communications is important in order to ensure that critical evidence is not lost. Obtaining copies of these past communications (e.g., stored e-mail that has been sent or received) can reveal evidence of criminality.
The power of expedited preservation of computer data is intended to address these problems. Parties are therefore required to introduce a power to order the preservation of specified computer data as a provisional measure, whereby data will be preserved for a period of time as long as necessary, up to a maximum of 90 days, for the competent authorities to provide for subsequent renewal of the order. This does not mean that the data is disclosed to law enforcement authorities at the time of preservation. For this to happen, an additional measure of disclosure or a search has to be ordered. With respect to law enforcement, Article 16 and provides for a maximum period of time for lent misrepresentations. However, it is in

Paragraph 1 in order to ensure that critical data is not lost during often consuming traditional mutual legal assistance procedures that enable the requested Party to actually obtain the data and disclose it to the requesting Party. Expedited preservation of stored computer data (Article 16)

158. Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer data in connection with a specific criminal investigation or proceeding.

159. "Preservation" requires that data, which already exists in a stored form, be protected from anything that would cause its corruption or destruction; otherwise to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be "frozen" (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data. The reference does not specify how data should be preserved. It is left to the order, for example, business, health, personal or other records. The measures are to be established by Parties for use in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. "Traffic data" also provides a link between the measures in Article 16 and 17. Paragraph 2 specifies that where a Party gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person’s possession or control. Thus, the stored data may actually be in the possession of the person if it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, for the competent authorities to seek its disclosure." The domestic law of a Party should specify a maximum period of time for which data, subject to an order, must be preserved, and the order should specify the exact period of time that the specified data is to be preserved. The period of time should be as long as necessary, up to a maximum of 90 days, to permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or the issuance of a production order, to obtain the disclosure of the data. A Party may provide for subsequent renewal of the production order. In this context, reference should be made to Article 29, which concerns a mutual assistance request to obtain the expeditious preservation of data stored by means of a computer system. That article specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data." Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertex may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order to ensure that other persons do not attempt to tamper with or delete the data. The person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data. In addition to the limitations set out above, the powers and procedures referred to in Article 16 are also subject to the conditions and safeguards provided in Articles 14 and 15.

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for a maximum of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the
proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specific communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, a court (in the absence of a separate preservation order on each service provider) may order the next service provider in the chain of the existence and terms of the preservation order. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.

Title 3 – Production order

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, or a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers.
For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards, to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be handled in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile or fixed line), services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address).

Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services.

Title 4 – Search and seizure of stored computer data

Search and seizure of stored computer data (Article 19)

184. This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law may provide for search and seize...
search and in respect of data that exists at that time. The
preconditions for obtaining legal authority to undertake a
search remain the same. The degree of belief required for
obtaining legal authorisation to search is not any different
whether the data is in tangible form or in electronic form.
Likewise, the belief and the search are in respect of data that
already exists and that will afford evidence of a specific
offence.

187. However, with respect to the search of computer data,
additional procedural provisions are necessary in order to
ensure that computer data can be obtained in a manner that is
equally effective as a search and seizure of a tangible data
carrier. There are several reasons for this: first, the data is in
intangible form, such as in an electromagnetic form. Second,
while the data may be read with the use of computer
equipment, it cannot be seized and taken away in the same
sense as can a paper record. The physical medium on which
the intangible data is stored (e.g., the computer hard-drive or a
diskette) must be seized and taken away, or a copy of the data
must be made in either tangible form (e.g., computer print-
out) or intangible form, on a physical medium (e.g., diskette),
before the tangible medium containing the copy can be seized
and taken away. In the latter two situations, where such copies
of the data are made, a copy of the data remains in the
computer system or storage device. Domestic law should
provide for a power to make such copies. Third, due to the
connectivity of computer systems, data may not be stored in the
primary computer that is searched, but such data may be
readily accessible to that system. It could be stored in an
associated data storage device that is connected directly to the
computer, or connected to the computer indirectly through
communication systems, such as the Internet. This may or may
not require new laws to permit an extension of the search to
where the data is actually stored (or the retrieval of the data
from that site to the computer being searched), or the use
traditional search powers in a more co-ordinated and
expeditious manner at both locations.

188. Paragraph 1 requires Parties to empower law
enforcement authorities to access and search computer data,
which is contained either within a computer system or part of
it (such as a connected data storage device), or on an
independent data storage medium (such as a CD-ROM or
diskette). As the definition of "computer system" in article 1
refers to "any device or a group of inter-connected or related
devices", paragraph 1 conceives the search of a computer
system and its related components that can be considered
together as forming one distinct computer system (e.g., a PC
together with a printer and related storage devices, or a local
area network). Sometimes data that is physically stored in
another system or storage device can be legally accessed
through accessing data that is contained in the connected computer
and establishing a connection with other distinct computer systems.
This situation, involving linkages with other computer systems by
means of telecommunication networks within the same
territory (e.g., wide area network or Internet), is addressed at
paragraph 2.

189. Although search and seizure of a "computer-data storage
medium in which computer data may be stored" (paragraph 1
(b)) may be undertaken by use of traditional search powers,
the execution of a computer search requires both the
search of the computer system and any related computer-data
storage medium (e.g., diskette) in the immediate vicinity of
the computer system. Due to this relationship, a
comprehensive legal authority is provided in paragraph 1 to
encompass both situations.

190. Article 19 applies to stored computer data. In this
respect, the question arises whether an unopened e-mail
message waiting in the mailbox of an ISP until the addressee
will download it to his or her computer system, has to be
considered as stored computer data or as data in transfer.
Under the law of some Parties, that e-mail message is part of
a communication and therefore its content can only be obtained
by applying the power of interception, whereas other legal
systems consider such message as stored data to which article
19 applies. Therefore, Parties should review their laws with
respect to this issue to determine what is appropriate within
their domestic legal systems.

191. Reference is made to the term ‘search or similarly access’.
The use of the traditional word ‘search’ conveys the idea of the
exercise of coercive power by the State, and indicates that the
power referred to in this article is analogous to traditional
search. ‘Search’ means to seek, read, inspect or review data. It
includes the notions of searching for data and searching of
(examining) data. On the other hand, the word ‘access’ has a
neutral meaning, but it reflects more accurately computer
terminology. Both terms are used in order to marry the
traditional concepts with modern terminology.

192. The reference to ‘in its territory’ is a reminder that this
provision, as all the articles in this Section, concern only
measures that are required to be taken at the national level.

193. Paragraph 2 allows the investigating authorities to
extend their search or similar access to another computer
system or part of it if they have grounds to believe that
the data required is stored in that other computer system. The
other computer system or part of it must, however, also be ‘in
its territory’.

194. The Convention does not prescribe how an extension of a
search is to be permitted or undertaken. This is left to
domestic law. Some examples of possible conditions are:
empowering the judicial or other authority which authorised
the computer search of a specific computer system, to
authorise the extension of such a search to a connected computer
system if he or she has grounds to believe (to the
degree required by national law and human rights safeguards)
that the connected computer system may contain the specific
data that is being sought; empowering the investigative
authorities to extend an authorised search or similar access of
a specific computer system to a connected computer system
where there are similar grounds to believe that the specific
data being sought is stored in the other computer system; or
exercising search or similar access powers at both locations in
a co-ordinated and expeditious manner. In all cases the data to
be searched must be lawfully accessible from or available to
the initial computer system.

195. This article does not address ‘transborder search and
seizure’, whereby States could search and seize data in the
territory of other States without having to go through the
usual channels of mutual legal assistance. This issue is
discussed below at the Chapter on international co-operation.

196. Paragraph 3 addresses the issues of empowering
competent authorities to seize or similarly secure computer
data that has been searched or similarly accessed under
paragraphs 1 or 2. This includes the power of seizure of
computer hardware and computer-data storage media. In
certain cases, for instance when data is stored in unique
operating systems such that it cannot be copied, it is
unavoidable that the data carrier as a whole has to be seized.
This may also be necessary when the data carrier has to be
examined in order to retrieve from it older data which was
overwritten but which has, nevertheless, left traces on the
data carrier.

197. In this Convention, ‘seize’ means to take away the
physical medium upon which data or information is recorded,
or to make and retain a copy of such data or information.
‘Seize’ includes the use or seizure of programmes needed to
access the data being seized. As well as using the traditional
term ‘seize’, the term ‘similarly secure’ is included to reflect
other means by which intangible data is removed, rendered
inaccessible or its control is otherwise taken over in the
computer environment. Since the measures relate to stored
intangible data, additional measures are required by
competent authorities to secure the data; that is, maintain the
integrity of the data, or maintain the ‘chain of custody’ of
the data, meaning that the data which is copied or removed be
retained in the State in which they were found at the time of
the seizure and remain unchanged during the time of criminal
proceedings. The term refers to taking control over or the
taking away of data.
198. The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography. The term 'removal' is intended to express the idea that while the data is removed or rendered inaccessible, it is not destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

199. Thus, seize or similarly secure data has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it. The seizure does not imply a final deletion of the seized data.

200. Paragraph 4 introduces a coercive measure to facilitate the search and seizure of computer data. It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should proceed. This provision therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

201. This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.

202. The information that can be ordered to be provided is that which is necessary to enable the undertaking of a search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

203. Under paragraph 5 of this article, the measures are subject to conditions and safeguards provided for under domestic law on the basis of Article 15 of this Convention. Such conditions may include provisions relating to the engagement and financial compensation of witnesses and experts.

204. The drafters discussed further in the frame of paragraph 5 if interested parties should be notified of the undertaking of a search procedure. In the on-line world it may be less apparent that data has been searched and seized (copied) than that a seizure in the off-line world took place, where seized objects will be physically missing. The laws of some Parties do not provide for an obligation to notify in the case of a traditional search. For the Convention to require notification in respect of a computer search would create a discrepancy in the laws of these Parties. On the other hand, some Parties may consider notification as an essential feature of the measure, in order to maintain the distinction between computer search of stored data (which is generally not intended to be a surreptitious measure) and interception of flowing data (which is a surreptitious measure, see Articles 20 and 21). The issue of notification, therefore, is left to be determined by domestic law. If Parties consider a system of mandatory notification of persons concerned, it should be borne in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.

Title 5 – Real-time collection of computer data

205. Articles 20 and 21 provide for the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer system. The provisions address the real-time collection and real-time interception of such data by competent authorities, as well their collection or interception by service providers. Obligations of confidentiality are also addressed.

206. Interception of telecommunications usually refers to traditional telecommunications networks. These networks can include cable infrastructures, whether wire or optical cable, as well as inter-connections with wireless networks, including mobile telephone systems and microwave transmission systems. Today, mobile communications are facilitated also by a system of specific satellite networks. Computer networks may also consist of an independent fixed cable infrastructure, but are more frequently operated as a virtual network by connections made through telecommunication infrastructures, thus permitting the creation of computer networks or linkages of networks that are global in nature. The distinction between telecommunications and computer communications, and the distinctiveness between their infrastructures, is blurring with the increase of convergence of telecommunication and information technologies. Thus, the definition of 'computer system' in article 1 does not restrict the manner by which the devices or group of devices may be inter-connected. Articles 20 and 21, therefore, apply to specified communications transmitted by means of a computer system, which could include transmission of data or the communication through telecommunication networks before it is received by another computer system.

207. Articles 20 and 21 do not make a distinction between a publicity or a privately owned telecommunication or computer system or to the use of systems and communication services offered to the public or to closed user groups or private parties. The definition of 'service provider' in Article 1 refers to public and private entities that provide to users of their services the ability to communicate by means of a computer system.

208. This Title governs the collection of evidence contained in currently generated communications, which are collected at the time of the communication (i.e., 'real time'). The data are intangible in form (e.g., in the form of transmissions of voice or electronic impulses). The flow of the data is not significantly interfered with by the collection, and the communication reaches its intended recipient. Instead of a physical seizure of the data, a recording (i.e., a copy) is made of the data being communicated. The collection of this evidence takes place during a certain period of time. A legal authority to permit the collection is sought in respect of a future event (i.e., a future transmission of data).

209. The type of data that can be collected is of two types: traffic data and content data. 'Traffic data' is defined in Article 1 to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).
210. In many States, a distinction is made between the real-time interception of content data and real-time collection of traffic data in terms of both the legal prerequisites required to authorise such investigative measure and the offences in respect of which this measure can be employed. While recognising that both types of data may have associated privacy interests, many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message. Greater limitations may be imposed with respect to the real-time collection of content data than traffic data. To assist in recognising this distinction for these States, the Convention, while operationally acknowledging that the data is collected or recorded in both situations, refers normatively in the titles of the articles to the collection of traffic data as ‘real-time collection’ and the collection of content data as ‘real-time interception’.

211. In some States existing legislation makes no distinction between the collection of traffic data and the interception of content data, either because no distinction has been made in the law regarding differences in privacy interests or the technological collection techniques for both measures are very similar. Thus, the legal prerequisites required to authorise the undertaking of the measures, and the offences in respect of which the measures can be employed, are the same. This situation is also recognised in the Convention by the common operational use of the term ‘collect or record’ in the actual text of both Articles 20 and 21.

212. With respect to the real-time interception of content data, the law often prescribes that the measure is only available in relation to the investigation of serious offences or categories of serious offences. These offences are identified in domestic law as serious for this purpose often by being named in a list of applicable offences or by being included in this category by reference to a certain maximum sentence of incarceration that is applicable to the offence. Therefore, with respect to the interception of content data, Article 21 specifically provides that Parties are only required to establish the measure ‘in relation to a range of serious offences to be determined by domestic law’.

213. Article 20, concerning the collection of traffic data, on the other hand, is not so limited and in principle applies to any criminal offence covered by the Convention. However, Article 14, paragraph 3, provides that a Party may reserve the right to apply the measure only to offences or categories of offences specified in the reservation, provided that the range of offences or categories of offences is not more restricted than the range of offences to which it applies the measure of interception of content data. Nevertheless, where such a reservation is taken, the Party shall consider restricting such reservation so as to enable the broadest range of application of the measure of collection of traffic data.

214. For some States, the offences established in the Convention would normally not be considered serious enough to permit interception of content data or, in some cases, even the collection of traffic data. Nevertheless, such techniques are often crucial for the investigation of some of the offences established in the Convention, such as those involving illegal access to computer systems, and distribution of viruses and child pornography. The source of the intrusion or distribution, for example, cannot be determined in some cases without real-time collection of traffic data. In some cases, the nature of the communication cannot be discovered without real-time interception of content data. These offences, by their nature or the means of transmission, involve the use of computer technologies. The use of technological means should, therefore, be permitted to investigate these offences. However, due to the sensitivities surrounding the issue of interception of content data, the Convention leaves the scope of this measure to be determined by domestic law. As some countries legally assimilate the collection of traffic data with the interception of content data, a reservation possibility is permitted to restrict the applicability of the former measure, but not to an extent greater than a Party restricts the measure of real-time interception of content data. Nevertheless, Parties should consider applying the two measures to the offences established by the Convention in Section 1 of Chapter II, in order to provide an effective means for the investigation of these computer offences and computer-related offences.

215. The conditions and safeguards regarding the powers and procedures related to real-time interception of content data and real-time collection of traffic data are subject to Articles 14 and 15. As interception of content data is a very intrusive measure on private life, stringent safeguards are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual. In the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights and its subsequent case-law (see judgments in Klaus (5), Kruslin (6), Huvig (7), Malone (8), Halford (9), Lambert (10) cases). Some of these safeguards are applicable also to the collection of traffic data in real-time.

Real-time collection of traffic data (Article 20)

216. Often, historical traffic data may no longer be available or it may not be relevant as the intruder has changed the route of communication. Therefore, the real-time collection of traffic data is an important investigative measure. Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings.

217. Traditionally, the collection of traffic data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine the source or destination (e.g., telephone numbers) and related data (e.g., time, date and duration) of various types of illegal communications (e.g., criminal threats and harassment, criminal conspiracy, fraudulent misrepresentations) and of communications affording evidence of past or future crimes (e.g., drug trafficking, money laundering, economic crimes, etc.).

218. Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it also has greater potential for committing crimes involving detection so as to enable the broadest range of application of the measure of collection of traffic data. Likewise, as computers can store vast quantities of data, often of a private nature, the potential for harm, whether economic, social or personal, can be significant if the integrity of this data is interfered with. Furthermore, as the science of computer technology is founded upon the processing of data, both as an end product and as part of its operational function (e.g., execution of computer programs), any interference with this data can have disastrous effects on the proper operation of computer systems. When an illegal distribution of child pornography, illegal access to a computer system or interference with the normal functioning of a computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, it is necessary and crucial to trace the route of the communications back from the victim to the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not due to the sensitivity of the issue of purely traditional telecommunications. This investigative technique can correlate the time, date and source and destination of the suspect’s communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.
219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified 'communications' are in the plural, as traffic data in respect of several communications may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The communications in respect of which the traffic data may be collected, however, must be specified. Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

220. Subject to paragraph 2, Parties are obliged, under paragraph 1(a) to ensure that their competent authorities have the capacity to collect or record traffic data by technical means. The article does not specify technologically how the collection is to be undertaken, and no obligations in technical terms are defined.

221. In addition, under paragraph 1(b), Parties are obliged to ensure that their competent authorities have the power to compel a service provider to collect or to co-operate and assist the competent authorities in the collection or recording of such data. This obligation regarding service providers is applicable only to the extent that the collection or recording, or co-operation and assistance, is within the existing technical capability of the service provider. The article does not oblige service providers to collect or co-operate and assist the competent authorities in the collection or recording of such data, which they may have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems. However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to engage the necessary measures to engage such capability. For example, the system may be configured in such a manner, or computer programs may already be possessed by the service provider, which would permit such measures to be taken, but they are not ordinarily executed or used in the normal course of the service provider's operation. The article would require the service provider to engage or turn-on these features, as required by law.

222. As this is a measure to be carried out at national level, the measures referred to in paragraph 1(a) are not necessarily limited to the collection or recording of specified communications in the territory of the Party. Thus, in practical terms, the obligations are generally applicable where the service provider has some physical infrastructure or equipment on that territory capable of undertaking the measures, although this need not be the location of its main operations or headquarters. For the purposes of this Convention, it is understood that a communication is in a Party's territory if one of the communicating parties' human beings or computers is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory.

223. In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a)). Likewise, an obligation under paragraph 1(b)(ii) to co-operate and assist the competent authorities in the collection or recording of traffic data is senseless if the competent authorities are not empowered to collect or record themselves the traffic data. Additionally, in the situation of some local area networks (LANs), where no service provider may be involved, the only way for collection or recording to be carried out would be for the investigating authorities to do it themselves. Both measures in paragraphs 1 (a) and (b) do not have to be used each time, but the availability of both methods is required by the article.

224. This dual obligation, however, posed difficulties for certain States in which the law enforcement authorities were only able to intercept data in telecommunication systems through the assistance of a service provider, and not surreptitiously without at least the knowledge of the service provider. For this reason, paragraph 2 accommodates such a situation. Where a Party, due to the 'established principles of its domestic legal system', cannot adopt the measures referred to in paragraph 1(a), it may instead adopt a different approach, such as compelling service providers to provide the necessary technical facilities, to ensure the real-time collection of traffic data by law enforcement authorities. In such case, all of the other limitations regarding territory, specificity of communications and use of technical means still apply.

225. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation. Service providers and employees of a service provider must be aware that the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively.

226. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. This provision not only ensures the confidentiality of the investigation, but it also relieves the service provider of any contractual or other legal obligations to notify subscribers that data about them is being collected. Paragraph 3 may be effected by the creation of explicit obligations in the law. On the other hand, a Party may be able to ensure the confidentiality of the measure on the basis of other domestic legal provisions, such as the power to prosecute for obstruction of justice those persons who aid the criminals by telling them about the measure. Although a specific confidentiality requirement (with effective sanction in case of a breach) is a preferred procedure, the use of obstruction of justice offences can be an alternative means to prevent inappropriate disclosure and, therefore, also suffices to implement this paragraph. Where explicit obligations of confidentiality are created, these shall be subject to conditions and safeguards as provided in Articles 14 and 15. These safeguards or conditions should impose reasonable time periods for the duration of the obligation, given the surreptitious nature of the investigative measure.

227. As noted above, the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g., websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15. Interception of content data (Article 21)

228. Traditionally, the collection of content data in respect of telecommunication (e.g., telephone conversations) has been a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or...
fraudulent misrepresentations) and to collect evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.). Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Many of the computer crimes involve the transmission or communication of data as part of their commission; for example, communications sent to effect an illegal access of a computer system or the distribution of computer viruses. It is not possible to determine in real-time the harmful nature of these communications without intercepting the content of the message. Without the ability to determine and prevent the occurrence of criminality in progress, law enforcement would merely be left with investigating past and completed crimes where the damage has already occurred. Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications.

Paragraph 230. Most of the elements of this article are identical to those of Article 20. Therefore, the provisions concerning the collection or recording of traffic data, obligations to co-operate and assist, and obligations of confidentiality apply equally to the interception of content data. Due to the higher privacy interest associated with content data, the investigative measure is restricted to a range of serious offences to be determined by domestic law.

Paragraph 231. As set forth in the comments above on Article 20, the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data.

Section 3 – Jurisdiction

Jurisdiction (Article 22)

Paragraph 232. This Article establishes a series of criteria under which Contracting Parties are obliged to establish jurisdiction over the criminal offences enumerated in Articles 2-11 of the Convention.

Paragraph 233. Paragraph 1 letter a is based upon the principle of territoriality. Each Party is required to punish the commission of crimes established in this Convention that are committed in its territory. For example, a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.

Paragraph 234. Consideration was given to including a provision requiring each Party to establish jurisdiction over offences involving satellites registered in its name. The drafters decided that such a provision was unnecessary since unlawful communications involving satellites will invariably originate from and/or be received on earth. As such, one of the bases for a Party’s jurisdiction set forth in paragraph 1(a) – (c) will be available if the transmission originates or terminates in one of the locations specified therein. Further, to the extent the offence involving a satellite communication is committed by a Party’s national outside the territorial jurisdiction of the State, there will be a jurisdictional basis under paragraph 1(d).

Finally, the drafters questioned whether registration was an appropriate basis for asserting criminal jurisdiction since in many cases there would be no meaningful nexus between the offence committed and the State of registry because a satellite serves as a mere conduit for a transmission.

Paragraph 235. Paragraph 1, letter b and c are based upon a variant of the principle of territoriality. These letters require each Party to establish criminal jurisdiction over offences committed upon ships flying its flag or aircraft registered under its laws. This obligation is already implemented as a general matter in the laws of many States, since such ships and aircraft are frequently considered to be an extension of the territory of the State. This type of jurisdiction is most useful where the ship or aircraft is not located in its territory at the time of the commission of the crime, as a result of which Paragraph 1, letter a would not be available as a basis to assert jurisdiction.

If the crime is committed on a ship or aircraft that is beyond the territory of the flag State, there may be no other State that would be able to exercise jurisdiction barring this requirement. In addition, if a crime is committed aboard a ship or aircraft which is merely passing through the waters or airspace of another State, the latter State may face significant practical impediments to the exercise of its jurisdiction, and it is therefore useful for the State of registry to also have jurisdiction.

Paragraph 236. Paragraph 1, letter d is based upon the principle of nationality. The nationality theory is most frequently applied by States applying the civil law tradition. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. Under letter d, if a national commits an offence abroad, the Party is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the State in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State.

Paragraph 237. Paragraph 2 allows Parties to enter a reservation to the jurisdiction grounds laid down in paragraphs 1, letters b, c and d. However, no reservation is permitted with respect to the establishment of territorial jurisdiction under letter a, or with respect to the obligation to establish jurisdiction in cases falling under the principle of "aut dedere aut judicare" (extradite or prosecute) under paragraph 3, i.e., where the Party has refused to extradite the alleged offender. Unlike under letter d, however, no reservation is permitted with respect to jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of "Extradition", Article 24, paragraph 6 of this Convention.

Paragraph 238. The bases of jurisdiction set forth in paragraph 1 are not the exclusive. Paragraph 4 of this Article permits the Parties to establish, in conformity with their domestic law, other types of criminal jurisdiction as well.

Paragraph 239. In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplicate effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "as appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.

Chapter III – International cooperation

Paragraph 240. Chapter III contains a number of provisions relating to extradition and mutual legal assistance among the Parties.

Section 1 – General principles

Title 1 – General principles relating to international cooperation
General principles relating to international co-operation (Article 23)

241. Article 23 sets forth three general principles with respect to international co-operation under Chapter III.

242. Initially, the article makes clear that international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

243. Second, the general scope of the obligation to co-operate is set forth in Article 23: co-operation is to be extended to all criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, literae a-b), as well as to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable. However, it should be noted that Articles 24 (Extradition), 33 (Mutual assistance regarding the interception of content data) and 34 (Mutual assistance regarding the interception of content data) permit the Parties to provide for a different scope of application of these measures.

244. Finally, co-operation is to be carried out both "in accordance with the provisions of this Chapter and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation. This basic principle is explicitly reinforced in Articles 24 (Extradition), 25 (General principles relating to mutual assistance), 26 (Spontaneous information), 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), 28 (Confidentiality and limitation on use), 31 (Mutual assistance regarding accessing of stored computer data), 33 (Mutual assistance regarding the real-time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data).

Title II – Principles relating to extradition

Extradition (Article 24)

245. Paragraph 1 specifies that the obligation to extradite applies only to offences established in accordance with Articles 2-11 of the Convention that are punishable under the laws of the requesting Party concerned by deprivation of liberty for a period that may legally be imposed for a violation of the offence for which extradition is sought. The determination of whether an offence is extraditable does not hinge on the actual penalty imposed in the particular case at hand, but instead on the maximum period that may legally be imposed for such an offence.

246. At the same time, in accordance with the general principle that international co-operation under Chapter III should be carried out pursuant to instruments in force between the Parties, Paragraph 1 also provides that where a treaty on extradition or an arrangement on the basis of uniform or reciprocal legislation is in force between two or more Parties (see description of this term in discussion of Article 27 below) which provides for a different threshold for extradition, the threshold provided for in such treaty or arrangement shall apply. For example, many extradition treaties between European countries and non-European countries provide that an offence is extraditable only if the maximum penalty is greater than one year's imprisonment or there is a more severe penalty. In such cases, international extradition practitioners will continue to apply the normal threshold under their treaty practice in order to determine whether an offence is extraditable. Even under the European Convention on Extradition (ETS N° 24), reservations may specify a different minimum penalty for extradition.

247. Paragraph 2 provides that the offences described in paragraph 1 are to be deemed extraditable offences in any extradition treaty between or among the Parties, and are to be included in future treaties they may negotiate among themselves. This does not mean that extradition must be granted on every occasion on which a request is made but rather that the possibility of granting extradition of persons for such offences must be available. Under paragraph 5, Parties are able to provide for other requirements for extradition.

248. Under paragraph 3, a Party that would not grant extradition, either because it has no extradition treaty with the requesting Party or because the existing treaties would not cover a request made in respect of the offences established in accordance with this Convention, may use the Convention itself as a basis for surrendering the person requested, although it is not obligated to do so.

249. Where a Party, instead of relying on extradition treaties, utilises a general statutory scheme to carry out extradition, paragraph 4 requires it to include the offences described in Paragraph 1 among those for which extradition is available.

250. Paragraph 5 provides that the requested Party need not extradite if it is not satisfied that all of the terms and conditions provided for by the applicable treaty or law have been fulfilled. It is thus another example of the principle that co-operation shall be carried out pursuant to the terms of applicable international instruments in force between the Parties, reciprocal arrangements, or domestic law. For example, conditions and restrictions set forth in the European Convention on Extradition (ETS N° 24) and its Additional Protocols (ETS N°s 86 and 98) will apply to Parties to those agreements, and extradition may be refused on such bases (e.g. Article 3 of the European Convention on the Protection of Human Rights and Fundamental Freedoms), or differs from the Convention, or where the request is considered to be granted, or where the request is considered to be refused, or there is no other reason that the offence is extraditable.

251. Paragraph 6 applies the principle "aut dedere aut judicare" (extradite or prosecute). Since many States refuse extradition of their nationals, offenders who are found in the Party of which they are a national may avoid responsibility for a crime committed in another Party unless local authorities are obliged to take action. Under paragraph 6, if another Party has sought extradition of the offender, and extradition has been refused on the grounds that the offender is a national of the requested Party, the requested Party must, upon request of the requesting Party, submit the case to its authorities for the purpose of prosecution. If the Party whose extradition request has been refused does not request submission of the case for local investigation and prosecution, there is no obligation on the requested Party to take action. Moreover, if no extradition request has been made, or if extradition has been denied on grounds other than nationality, this paragraph establishes no obligation on the requested Party to submit the case for domestic prosecution. In addition, paragraph 6
requires the local investigation and prosecution to be carried out with diligence; it must be treated as seriously "as in the case of any other offence of a comparable nature" in the Party submitting the case. That Party shall report the outcome of its investigation and proceedings to the Party that had made the request for assistance.

252. In order that each Party know to whom its requests for provisional arrest or extradition should be directed, paragraph 7 requires Parties to communicate to the Secretary General of the Council of Europe the name and address of its authorities responsible for making requests for extradition or provisional arrest in the absence of a treaty. This provision has been limited to situations in which there is no extradition treaty in force between the Parties concerned because if a bilateral or multilateral extradition treaty is in force between the Parties (such as ETS No. 24), the Parties will know to whom extradition and provisional arrest requests are to be directed without the necessity of a registration requirement. The communication to the Secretary General must be made at the time of signature or when depositing the Party's instrument of ratification, acceptance, approval or accession. It should be noted that designation of an authority does not exclude the possibility of using the diplomatic channel.

Title 3 – General principles relating to mutual assistance

General principles relating to mutual assistance (Article 25)

253. The general principles governing the obligation to provide mutual assistance are set forth in paragraph 1. Cooperation is to be provided "to the widest extent possible." Thus, as in Article 23 ("General principles relating to international co-operation"), mutual assistance is in principle to be extensive, and impediments thereto strictly limited. Second, as in Article 23, the obligation to co-operate applies in principle to both criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, letter a-b), and to the collection of evidence in electronic form of a criminal offence. It was agreed to impose an obligation to co-operate as to this broad class of crimes because there is the need for streamlined mechanisms of international co-operation as to both of these categories. However, Articles 34 and 35 permit the Parties to provide for a different scope of application of these measures.

254. Other provisions of this Chapter will clarify that the obligation to provide mutual assistance is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements. Under paragraph 2, each Party is required to have a legal basis to carry out the specific forms of co-operation described in the remainder of the Chapter, if its treaties, laws and arrangements do not already contain such provisions. The availability of such mechanisms, either in the treaty or in domestic law, similar to those contained in the treaties, laws and arrangements, would provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance. For example, an intrusive measure, such as search and seizure, is not executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such measure are satisfied. The requested Party also may ensure protection of rights of persons in relation to the items seized and provided through mutual legal assistance.

255. Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. In paragraph 1, co-operation is to be provided "to the widest extent possible." This clause is designed to signal that the Convention contains several significant exceptions to the general principle. The first such exception has been seen in paragraph 2 of this Article, which obliges each Party to provide for the forms of co-operation set forth in the remaining articles of the Chapter (such as preservation, real time collection of data, search and seizure, and maintenance of a 24/7 network), regardless of whether or not its MLATs, equivalent arrangements or mutual assistance laws currently provide for such measures. Another exception is found in Article 27 which is always to be applied to the execution of requests in lieu of the requested Party's domestic laws. Co-operation in the sense of an MLAT or equivalent arrangement between the requesting and requested Parties. Article 27 provides a system of conditions and grounds for refusal. Another exception, specifically provided for in this paragraph, is that co-operation may not be denied, at least as far as the offences established in Articles 2 – 11 of the Convention are concerned, on the grounds that the requested Party considers the request to involve a "fiscal" offence. Finally, Article 29 is an exception in that it provides that preservation may not be denied on dual criminality grounds, although the possibility of a reservation is provided for in this respect.

259. Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance (for example, where a requested Party has reserved its right to require dual criminality with respect to the preservation of data under Article 29, paragraph 4 "Expeditied preservation of stored computer data), dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in
denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in national legal systems, variations in terminology and categorisation of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance.

Spontaneous (Article 26)

260. This article is derived from provisions in earlier Council of Europe instruments, such as Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141) and Article 28 of the Criminal Law Convention on Corruption (ETS N° 173). More and more frequently, a Party possesses valuable information that it believes may assist another Party in a criminal investigation or proceeding, and which the Party conducting the investigation or proceeding is not aware exists. In such cases, no request for mutual assistance will be forthcoming. Paragraph 1 empowers the State in possession of the information to forward it to the other State without a prior request. The provision was thought useful because, under the laws of some States, such a positive grant of legal authority is needed in order to provide assistance in the absence of a request. A Party is not obligated to spontaneously forward information to another Party; it may exercise its discretion in light of the circumstances of the case at hand. Moreover, the spontaneous disclosure of information does not preclude the disclosing Party, if it has jurisdiction, from investigating or instituting proceedings in relation to the facts disclosed.

261. Paragraph 2 addresses the fact that in some circumstances, a Party will only forward information spontaneously if sensitive information will be kept confidential or other conditions can be imposed on the use of the information. In particular, confidentiality will be an important consideration in cases in which important interests of the providing State may be endangered should the information be made public, e.g., where there is a need to protect the identity of a means of collecting the information or the fact that a criminal group is being investigated. If advance inquiry reveals that the receiving Party cannot comply with a condition sought by the providing Party (for example, where it cannot comply with obligations concerning confidentiality because the information is needed as evidence at a public trial), the receiving Party shall advise the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it. It is foreseen that conditions imposed under this article are derived from provisions in earlier Council of Europe instruments, such as Article 25, paragraph 1, authorising the providing Party to request mutual assistance from the receiving Party.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Proceedures pertaining to mutual assistance requests in the absence of applicable international agreements (Article 27)

262. Article 27 obliges the Parties to apply certain mutual assistance procedures and conditions where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties. The Article 27 conditions are consistent with those that could be imposed by the providing Party pursuant to a request for mutual assistance from the receiving Party.

mechanisms particularly necessary for rapid effective cooperation in computer related criminal matters, such as those in Articles 29-35 (Specific provisions – Title 1, 2, 3) is each Party required to establish a legal basis to enable the carrying out of such forms of co-operation if its current mutual assistance treaties, arrangements or laws do not already do so. 263. Accordingly, most forms of mutual assistance under this Chapter will continue to be carried out pursuant to the European Convention on Mutual Assistance in Criminal Matters (ETS N° 30) and its Protocol (ETS N° 99) among the Parties. Alternatively, Parties to this Convention that have bilateral MLATs in force between them, or other multilateral agreements governing mutual assistance in criminal cases (such as between member States of the European Union), shall continue to apply their terms, supplemented by the computer- or computer-related crime-specific mechanisms described in the remainder of Chapter III, unless they agree to apply any or all of the provisions of this Article in lieu thereof. Mutual assistance may also be based on arrangements agreed on the basis of uniform or reciprocal legislation, such as the system of co-operation developed among the Nordic countries, which is also admitted by the European Convention on Mutual Assistance in Criminal Matters (Article 25, paragraph 4), and among members of the Commonwealth. Finally, the reference to mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation is not limited to those instruments in force at the time of entry into force of this present Convention, but also covers instruments that may be adopted in the future.

264. Article 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), paragraphs 2-10, provide a number of rules for providing mutual assistance in the absence of an MLAT or arrangement on the basis of uniform or reciprocal legislation, including establishment of central authorities, imposing of conditions, grounds for and procedures in cases of postponement or refusal, confidentiality of requests, and direct communications. With respect to such expressly covered issues, in the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the provisions of this Article are to be applied in lieu of otherwise applicable domestic laws governing mutual assistance. At the same time, Article 27 does not provide rules for other issues typically dealt with in domestic legislation governing international mutual assistance. For example, there are no provisions dealing with the form and contents of requests, taking of witness testimony in the requested or requesting Parties, the providing of official documents, transfer of witnesses in custody, or assistance in confiscation matters. With respect to such issues, Article 25, paragraph 1, authorises the Parties to apply, in the case of the provisions of this Chapter, the law of the requested Party shall govern specific modalities of providing that type of assistance. 265. Paragraph 2 requires the establishment of a central authority or authorities responsible for sending and answering requests for assistance. The institution of central authorities is a common feature of modern instruments dealing with mutual assistance in criminal matters, and it is particularly helpful in ensuring the kind of rapid reaction that is so useful in combating computer- or computer-related crime. Initially, direct transmission between such authorities is slower than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign legal authorities, and that requests, particularly urgent or sensitive requests are dealt with promptly.

266. Parties are encouraged as a matter of efficiency to designate a single central authority for the purpose of mutual assistance; it would generally be most efficient for the authority designated for such purpose under a Party’s MLATs, or domestic law to also serve as the central authority when
this article is applicable. However, a Party has the flexibility to designate more than one central authority where this is appropriate under its system of mutual assistance. Where more than one central authority is established, the Party that has done so should ensure that each authority interprets the provisions of the Convention in the same way, and that both incoming and outgoing requests are treated rapidly and efficiently. Each Party is to advise the Secretary General of the Council of Europe of the names and addresses (including e-mail and fax numbers) of the authority or authorities designated to receive and respond to mutual assistance requests under this Article, and Parties are obliged to ensure that the designation is kept up-to-date. 267. A major objective of a State requesting mutual assistance often is to ensure that its domestic laws governing the admissibility of evidence are fulfilled, and it can use the evidence before its courts as a result. To ensure that such evidentiary requirements can be met, paragraph 3 obliges the requested Party to execute requests in accordance with the procedures specified by the requesting Party, unless to do so would be incompatible with its law. It is emphasised that this paragraph relates only to the obligation to respect technical procedural requirements, not to fundamental procedural protections. Thus, for example, a requesting Party cannot require the requested Party to execute a search and seizure that would not meet the requested Party’s fundamental legal requirements for this measure. In light of the limited nature of the obligation, it was agreed that the requested Party’s legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party; instead, the procedure must be incompatible with the requested Party’s legal principles. For example, under the law of the requesting Party, it may be a procedural requirement that a statement of a witness be given under oath. Even if the requested Party does not domestically have the requirement that statements be given under oath, it should honour the requesting Party’s request. 268. Paragraph 4 provides for the possibility of refusing requests for mutual assistance requests brought under this Article. Assistance may be refused on the grounds provided for in Article 25, paragraph 4 (i.e. grounds provided for in the law of the requested Party), including prejudice to the sovereignty of the State, security, ordre public or other essential interests, and where the offence is considered by the requested Party’s legal system to be a political offence or an offence connected with a political offence. In order to promote the overriding principle of providing the widest measure of cooperation (see Articles 23, 25), grounds for refusal established by a requested Party should be narrow and exercised with restraint. They may not be so expansive as to create the potential for abuse or to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information. 269. In line with this approach, it was understood that apart from those grounds set out in Article 28, refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties to be considered by the requested Party to fall within the essential interests ground of refusal. A broad, categorical, or systematic application of data protection principles to refuse cooperation is therefore precluded. Thus, the fact the Parties concerned have different systems of protecting the privacy of data (such as that the requesting Party does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting Party uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities) do not as such constitute grounds for refusal. Before invoking “essential interests” as a basis for refusing co-operation, the requested Party should instead attempt to place conditions which would allow the transfer of the data. (see Article 27, paragraph 6 and paragraph 271 of this report). 270. Paragraphs 5 permits the requesting Party to postpone, rather than refuse, assistance where immediate action on the request would be prejudicial to investigations or proceedings in the requested Party. For example, where the requesting Party has sought to obtain evidence or witness testimony for purposes of investigation or trial, and the same evidence or witness are needed at a trial that is about to commence in the requested Party, the requested Party would be justified in postponing the providing of assistance. 271. Paragraph 6 provides that where the assistance sought would otherwise be refused or postponed, the requested Party may instead provide assistance subject to conditions. If the conditions are not agreeable to the requesting Party, the requested Party may modify them, or it may exercise its right to refuse or postpone assistance. Since the requested Party has an obligation to provide the widest possible measure of assistance, it was agreed that both grounds for refusal and conditions should be exercised with restraint. 272. Paragraph 7 obliges the requested Party to keep the requesting Party informed of the outcome of the request, and requires reasons to be given in the case of refusal or postponement of assistance. The providing of reasons can, inter alia, assist the requesting Party to understand how the requested Party interprets the requirements applicable, provide a basis for consultation in order to improve the future efficiency of mutual assistance, and provide to the requesting Party previously unknown factual information about the availability or condition of witnesses or evidence. 273. There are times when a Party makes a request in a particularly sensitive case, or in a case in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely. Paragraph 8 accordingly permits the requesting Party to request that the fact and content of the request be kept confidential. Confidentiality may not be sought, however, to the extent that it would undermine the requested Party’s ability to obtain the evidence or information sought, e.g., where the information will need to be disclosed in order to obtain a court ordered need to effect assistance, or where private persons possessing evidence will need to be made aware of the request in order for it to be successfully executed. If the requested Party cannot comply with the request for confidentiality, it shall notify the requesting Party, which then has the option of withdrawing or modifying the request. 274. Central authorities designated in accordance with paragraph 2 shall communicate directly with one another. However, in case of urgent requests for mutual legal assistance may be sent directly by judges and prosecutors of the requesting Party to the judges and prosecutors of the requested Party. The judge or prosecutor following this procedure must also address a copy of the request made to his own central authority with a view to its transmission to the central authority of the requested Party. Under littera b, requests may be channeled through Interpol. Authorities of the requested Party that receive a request falling outside their field of competence, are, pursuant to littera c, under a two-fold obligation. First, they must transfer the request to the competent authority of the requested Party. Second, the requesting Party must inform the authorities of the requested Party of the transfer made. Under littera d, requests may also be transmitted directly without the intervention of central authorities even if there is no urgency, as long as the authority of the requested Party is able to comply with the request without making use of coerc as that the relevant litteras enable a Party to inform others, through the Secretary General of the Council of Europe, that, for reasons of efficiency, direct communications are to be addressed to the central authority. Confidentiality and limitation on use (Article 28) 275. This provision specifically provides for limitations on use of information or material, in order to enable the requested
Party, in cases in which such information or material is particularly sensitive, to ensure that its use is limited to that for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting Party. These restrictions provide safeguards that are available for inter alia data protection purposes.

276. As in the case of Article 27, Article 28 only applies where there is no mutual assistance treaty, or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties. Where such treaty or arrangement is in force, its provisions on confidentiality and use limitations shall apply in lieu of the provisions of this Article, unless the Parties thereto agree otherwise. This avoids overlap with existing bilateral and multilateral mutual legal assistance treaties (MLATs) and similar arrangements, thereby enabling practitioners to continue to operate under the normal well-understood regime rather than seeking to apply two competing, possibly contradictory, instruments.

277. Paragraph 2 allows the requested Party, when responding to a request for mutual assistance, to impose two types of conditions. First, it may request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such condition, such as where the identity of a confidential informant is involved. It is not appropriate to require absolute confidentiality in cases in which the requested Party is obligated to provide the requested assistance, as this would, in many cases, thwart the ability of the requesting Party to successfully investigate or prosecute crime, e.g., by using the evidence in a public trial (including compulsory disclosure).

278. Second, the requested Party may make furnishing of the information or material dependent on the condition that it not be used for investigations or proceedings other than those stated in the request. In order for this condition to apply, it must be expressly invoked by the requested Party, otherwise, there is no such limitation on use by the requesting Party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested Party. Two exceptions to the ability to limit use were recognised by the negotiators and are implicit in the terms of the paragraph. First, under fundamental legal principles of many States, if material furnished is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, most material furnished under mutual assistance regimes is intended for use at trial, normally a public proceeding (including compulsory disclosure). Once such disclosure takes place, the material has essentially passed into the public domain. In these situations, it is not possible to limit the confidentiality of the information or material. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the prosecution of the offence concerned and that preservation is required to enable preservation of the data. In order for this condition to apply, it must be expressly invoked by the requested Party, otherwise, there is no such limitation on use by the requesting Party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested Party. Two exceptions to the ability to limit use were recognised by the negotiators and are implicit in the terms of the paragraph. First, under fundamental legal principles of many States, if material furnished is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, most material furnished under mutual assistance regimes is intended for use at trial, normally a public proceeding (including compulsory disclosure). Once such disclosure takes place, the material has essentially passed into the public domain. In these situations, it is not possible to limit the confidentiality of the information or material. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the prosecution of the offence concerned and that preservation is required to enable preservation of the data. In order for this condition to apply, it must be expressly invoked by the requested Party, otherwise, there is no such limitation on use by the requesting Party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested Party. Two exceptions to the ability to limit use were recognised by the negotiators and are implicit in the terms of the paragraph. First, under fundamental legal principles of many States, if material furnished is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, most material furnished under mutual assistance regimes is intended for use at trial, normally a public proceeding (including compulsory disclosure). Once such disclosure takes place, the material has essentially passed into the public domain. In these situations, it is not possible to limit the confidentiality of the information or material.
territory, but may not until later have a good understanding of the nature and extent of damage. If the requested Party were to delay preserving traffic data that would trace the source of the intrusion pending conclusive establishment of dual criminality, the critical data would often be routinely deleted by service providers holding it for on hospitalizing the transmission has been made. Even if thereafter the requesting Party were able to establish dual criminality, the crucial traffic data could not be recovered and the perpetrator of the crime would never be identified.

Accordingly, the general rule is that Parties must dispense with any dual criminality requirement for the purpose of preservation. However, a limited reservation is available under paragraph 4. If a Party requires dual criminality as a condition for responding to a request for mutual assistance for production of the data, and if it has reason to believe that, at the time of disclosure, dual criminality will not be satisfied, it may reserve the right to require dual criminality as a precondition to preservation. With respect to offences established in accordance with Articles 2 through 11, it is assumed that the condition of dual criminality is automatically met between the Parties, subject to any reservations they may have entered to these offences where permitted by the Convention. Therefore, Parties may impose this requirement only in relation to offences other than those defined in the Convention.

287. Otherwise, under paragraph 5, the requested Party may only refuse a request for mutual assistance where the party considering whether to disclose the traffic data, where execution will prejudice its sovereignty, security, ordre public or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. Due to the centrality of this measure to the effective investigation and prosecution of computer-related crime, it was agreed that the assertion of any other basis for refusing a request for preservation is precluded.

288. At times, the requested Party will realise that the custodian of the data is likely to take action that will threaten the confidentiality of, or otherwise prejudice, the requesting Party’s investigation (for example, where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of the investigation himself). In such situations, under paragraph 6, the requesting Party must be notified promptly, so that it may assess whether to take the risk posed by carrying through with the request for preservation, or whether to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.

289. Finally, paragraph 7 obliges each Party to ensure that data preserved pursuant to this Article will be held for at least 60 days pending receipt of a formal mutual assistance request seeking the disclosure of the data, and continue to be held following receipt of the request.

Expedited disclosure of preserved traffic data (Article 30)

290. This article provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed through a service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting Party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.

291. Under Paragraph 2, the requested Party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, ordre public or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 19 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.

Title 2 – Mutual assistance regarding investigative powers

Mutual assistance regarding accessing of stored computer data (Article 31)

292. Each Party must have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory – just as under Article 19 (Search and seizure of stored computer data) it must have the ability to do so for domestic purposes. Paragraph 1 authorises a Party to request this type of mutual assistance, and paragraph 2 requires the requested Party to be able to provide it. Paragraph 2 also follows the principle that the terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters. Under paragraph 3, such a request must be responded to on an expedited basis where (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or (2) otherwise where such treaties, arrangements or laws so provide.

Transborder access to stored computer data with consent or where publicly available (Article 32)

293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.

294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person’s e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

Mutual assistance regarding the real-time collection of traffic data (Article 33)
In many cases, investigators cannot ensure that they are able to trace a communication to its source by following the trail through records of prior transmissions, as key traffic data may have been automatically deleted by a service provider in the chain of transmission before it could be preserved. It is therefore critical for investigators in each Party to have the ability to obtain traffic data in real time regarding communications passing through a computer system in other Parties. Accordingly, under Article 33 (Mutual assistance regarding the real-time collection of traffic data), each Party is under the obligation to collect traffic data in real time for another Party. While this Article requires the Parties to cooperate on these matters, here, as elsewhere, deference is given to existing modalities of mutual assistance. Thus, the terms and conditions by which such co-operation is to be provided are generally those set forth in applicable treaties, arrangements and laws governing mutual legal assistance in criminal matters.

In many countries, mutual assistance is provided broadly with respect to the real time collection of traffic data, because such collection is viewed as being less intrusive than either interception of content data, or search and seizure. However, a number of States take a narrower approach. Accordingly, in the same way as the Parties may enter a reservation under Article 14 (Scope of procedural provisions), paragraph 3, with respect to the scope of the equivalent domestic measure, paragraph 2 permits Parties to limit the scope of application of this measure to offences for which provision is made to in Article 23 (General principles relating to international co-operation). One caveat is provided: in no event may the range of offences be more narrow than the range of offences for which such measure is available in an equivalent domestic case. Indeed, because real time collection of traffic data is at times the only way of ascertaining the identity of the perpetrator of a crime, and because of the lesser intrusiveness of the measure, the use of the term "at least" in paragraph 2 is designed to encourage Parties to permit as broad assistance as possible, i.e., even in the absence of dual criminality.

Mutual assistance regarding the interception of content data (Article 34)

Because of the high degree of intrusiveness of interception, the obligation to provide mutual assistance for interception of content data is restricted. The assistance is to be provided to the extent permitted by the Parties' applicable treaties and laws. As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, it was decided to defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist. In this regard, reference is made to Standing Committee of Experts conclusions elaborated within the framework of the Council of Europe, for instance, the Convention on the Transfer of Sentenced Persons (ETS No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications.

Final provisions

Title 3 – 24/7 Network

24/7 Network (Article 35)

As has been previously discussed, effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. Moreover, with a few keystrokes, action may be taken in one part of the world that instantly has consequences many thousands of kilometres and many time zones away. For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in this Article is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under this Article, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of this Chapter, in particular as defined under Article 35, paragraph 1, litterae a) – c). It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime.

Each Party's 24/7 point of contact is to facilitate or directly carry out, inter alia, the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. The term "legal information" in Paragraph 1 means advice to another Party that is seeking co-operation of any legal prerequisites required for providing technical assistance or formal co-operation. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer- or computer-related crime, yet other choices may be appropriate for a particular Party, given its governmental structure and legal system. Since the 24/7 contact is to provide both technical advice for stopping or tracing an attack as well as such international co-operation duties as locating of suspects, there is no one correct answer, and it is anticipated that the structure of the network will evolve over time. In designating the national point of contact, due consideration should be given to the need to communicate with points of contacts using other languages.

Article 36, paragraph 1, requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis.

Paragraph 3 requires each point of contact in the network to have proper equipment. Up-to-date telephone, fax and computer equipment will be essential to the smooth operation of the network, and other forms of communication and analytical equipment will need to be part of the system as technology advances. Paragraph 3 also requires that personnel participating as part of a Party's team for the network be properly trained regarding computer- or computer-related crime and how to respond to it effectively.

Chapter IV – Final provisions

With some exceptions, the provisions contained in this Chapter are, for the most part, based on the Model final clauses for conventions contained in Article 35 and 21 as well as on the Standing Committee of Experts conclusions elaborated within the framework of the Council of Europe which were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980. As most of the articles 36 through 48 either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe, they do not call for specific comments. However, certain modifications of the standard model clauses or some new provisions require some explanation. It is noted in this context that the model clauses have been adopted as a non-binding set of provisions. As the Introduction to the Model Clauses pointed out, "these final clauses are only intended to facilitate the task of committees of experts and avoid textual divergences which would not have any real justification. The model is in no way binding and different clauses may be adapted to fit particular cases."

Signature and entry into force (Article 36)

Article 36, paragraph 1, has been drafted following several precedents established in other conventions elaborated within the framework of the Council of Europe, for instance, the Convention on the Transfer of Sentenced Persons (ETS No. 112) and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141), which allow for signature, before their entry into force,
not only by the member States of the Council of Europe, but also by non-member States which have participated in their elaboration. The provision is intended to enable the maximum number of interested States, not just members of the Council of Europe, to become Parties as soon as possible. Here, the provision is intended to apply to four non-member States: Canada, Japan, South Africa and the United States of America, which actively participated in the elaboration of the Convention. Once the Convention enters into force, in accordance with paragraph 3, other non-member States not covered by this provision may be allowed to accede to the Convention in conformity with Article 37, paragraph 1.

305. Article 36, paragraph 3 sets the number of ratifications, acceptances or approvals required for the Convention's entry into force at 5. This figure is higher than the usual threshold (3) in Council of Europe treaties and reflects the belief that a slightly larger group of States is needed to successfully begin addressing the challenge of international computer- or computer-related crime. The number is not so high, however, so as not to delay unnecessarily the Convention's entry into force. Among the five initial States, at least three must be Council of Europe members, but the two others could come from the four non-member States that participated in the Convention's elaboration. This provision would of course also allow for the Convention to enter into force based on expressions of consent to be bound by five Council of Europe member States.

306. Article 37 has also been drafted on precedents established in other Council of Europe conventions, but with an additional express element. Under long-standing practice, the Committee of Ministers decides, on its own initiative or upon request, to invite a non-member State, which has not participated in the elaboration of a convention, to accede to the convention after having consulted all contracting Parties, whether member States or not. This implies that if any contracting Party objects to the non-member State's accession, the Committee of Ministers would usually not invite it to join the convention. However, under the usual formulation, the Committee of Ministers could – in theory – invite such a non-member State to accede to a convention even if a non-member State Party objected to its accession. This means that – in theory – no right of veto is usually granted to non-member States Parties in the process of extending Council of Europe treaties to other non-member States. However, an express requirement that the Committee of Ministers consult with and obtain the unanimous consent of all Contracting States – not just members of the Council of Europe – before inviting a non-member State to accede to the Convention has been inserted. As indicated above, such a requirement is consistent with principle and recognises that extending States to the Convention should be able to determine with which non-member States they are to enter into treaty relations. Nevertheless, the formal decision to invite a non-member State to accede will be taken, in accordance with usual practice, by the representatives of the contracting Parties entitled to sit on the Committee of Ministers. This decision requires the two-thirds majority provided for in Article 20.d of the Statute of the Council of Europe and the unanimous vote of the representatives of the contracting Parties entitled to sit on the Committee.

307. Federal States seeking to accede to the Convention, which intend to make a declaration under Article 41, are required to submit in advance a draft of the statement referred to in Article 41, paragraph 3, so that the Parties will be in a position to evaluate how the application of the federal clause would affect the prospective Party's implementation of the Convention (see paragraph 320).

Effects of the Convention (Article 39)

308. Article 39, paragraphs 1 and 2 address the Convention's relationship to other international agreements or arrangements. The subject of how conventions of the Council of Europe should relate to one another or to other treaties, bilateral or multilateral, concluded outside the Council of Europe is not dealt with by the Model Clauses referred to above. The usual approach utilised in Council of Europe conventions in the criminal law area (e.g., Agreement on Illicit Traffic by Sea (ETS No. 156)) is to provide that: (1) new conventions do not affect the rights and undertakings derived from existing treaties; (2) Parties will apply relevant international agreements and arrangements between Parties and it mentions in particular three Council of Europe treaties as non-exhaustive examples: the 1957 European Convention on Extradition (ETS No. 24), the 1959 European Convention on Criminal Matters (ETS No. 30) and its 1978 Additional Protocol (ETS No. 99). Therefore, regarding general matters, such agreements or arrangements should in principle be applied by the Parties to the Convention on cybercrime. Regarding specific matters only dealt with by this Convention, the rule of interpretation lex specialis derogat legi generali provides that the Parties should give precedence to the rules contained in the Convention. An example is Article 30, which provides for the expedited disclosure of preserved traffic data when necessary to identify the path of a specified communication. In this specific area, the Convention, as lex specialis, should provide a rule of first resort over provisions in more general mutual assistance agreements.

310. Similarly, the drafters considered language making the application of existing or future agreements contingent on whether they "strengthen" or "facilitate" co-operation as possibly problematic, because, under the approach established in the international co-operation Chapter, the presumption is that Parties will apply relevant international agreements and arrangements.

311. Where there is an existing mutual assistance treaty or arrangement as a basis for co-operation, the present Convention would only supplement, where necessary, the existing rules. For example, this Convention would provide for the transmission of mutual assistance requests by expedited means of communications (see Article 25, paragraph 3) if such a possibility does not exist under the original treaty or arrangement.

312. Consistent with the Convention's supplementary nature and, in particular, its approach to international co-operation, paragraph 2 provides that Parties are also free to apply agreements that already exist or that may in the future come into force. Precedent for such an articulation is found in the Transfer of Sentenced Persons Convention (ETS No. 112). Certainly, in the context of international co-operation, it is expected that application of other international agreements (many of which offer proven, longstanding formulas for international assistance) will in fact promote co-operation. Consistent with the terms of the present Convention, Parties may also agree to apply its international co-operation provisions in lieu of such other agreements (see Article 27(1)). In such instances the relevant co-operation provisions set forth in Article 27 would supersede the relevant rules in such other agreements. As the present Convention generally
provides for minimum obligations, Article 39, paragraph 2 recognises that Parties are free to assume obligations that are more specific in addition to those already set out in the Convention, when establishing their relations concerning matters dealt with therein. However, this is not an absolute right: Parties must respect the objectives and principles of the Convention when so doing and therefore cannot accept obligations that would defeat its purpose.

313. Further, in determining the Convention’s relationship to other international agreements, the drafters also concurred that Parties may look for additional or relevant provisions in the Vienna Convention on the Law of Treaties. Therefore, paragraph 3 was inserted to make plain that the Convention only affects what it addresses. Left unaffected are other rights, restrictions, obligations and responsibilities that may exist but that are not dealt with by the Convention. Precedent for such a “savings clause” may be found in other international agreements (e.g., UN Terrorist Financing Convention).

314. While the Convention provides a much-needed level of harmonisation, it does not purport to address all outstanding issues relating to computer or computer-related crime. Therefore, paragraph 3 was inserted to make plain that the Convention only affects what it addresses. Left unaffected are other rights, restrictions, obligations and responsibilities that may exist but that are not dealt with by the Convention. Precedent for such a “savings clause” may be found in other international agreements (e.g., UN Terrorist Financing Convention).

Declarations (Article 40)

315. Article 40 refers to certain articles, mostly in respect of the offences established by the Convention in the substantive law section, where Parties are permitted to include certain specified additional elements which modify the scope of the provisions. Additional elements may be of a conceptual or legal differences, which in a treaty of global ambition are more justified than they perhaps might be in a purely Council of Europe context. Declarations are considered acceptable interpretations of Convention provisions and should be distinguished from reservations, which permit a Party to exclude or modify the legal effect of certain obligations set forth in the Convention. Since it is important for Parties to the Convention to know which, if any, additional elements have been attached by other Parties, there is an obligation to declare them to the Secretary General of the Council of Europe at the time of signature or when depositing an instrument of ratification, acceptance, approval or accession. Such notification is particularly important concerning the definition of offences, as the condition of dual criminality will have to be met by the Parties when applying certain procedural powers. No numerical limit was felt necessary in respect of declarations.

Federal clause (Article 41)

316. Consistent with the goal of enabling the largest possible number of States to become Parties, Article 41 allows for a reservation which is intended to accommodate the difficulties of some States in the context of certain aspects of their domestic law. In order to maintain their reservations in respect of certain provisions of the Convention, when making a reservation under paragraph 1 of Article 41, a Party must respect the objectives and principles of the Convention when so doing and therefore cannot accept obligations that would defeat its purpose.

317. For example, in the United States, under its Constitution and fundamental principles of federalism, federal criminal legislation generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by the constituent States. This approach to federalism still provides for broad coverage of illegal conduct encompassed by this Convention under US federal criminal law, but recognises that the constituent States would continue to regulate conduct that has only minor impact or is purely local in character. In some instances, within that narrow category of conduct regulated by State but not federal law, a constituent State may not provide for a measure that would otherwise fall within the scope of this Convention. For example, an attack on a stand-alone personal computer, or network of computers linked together in a single building, may only be penalised if provided for under the law of the State in which the attack took place; however the attack would be a federal offence if access to the computer took place through the Internet, since the use of the Internet provides the effect on interstate or foreign commerce necessary to invoke federal law. The implementation of this Convention through United States federal law, or through the law of another federal State under similar circumstances, would be in conformity with the requirements of Article 41.

318. The scope of application of the federal clause has been restricted to the provisions of Chapter I (substantive criminal law, procedural law and jurisdiction). Federal States making use of this provision would still be under the obligation to cooperate with the other Parties under Chapter III, even where the constituent State or other similar territorial entity in which a fugitive or evidence is located does not criminalise conduct or does not have procedures required under the Convention.

319. In addition, paragraph 2 of Article 41 provides that a federal State, when making a reservation under paragraph 1 of this Article, may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures that are intended to achieve a broad and effective law enforcement capability with respect to those measures. In respect of provisions the implementation of which come within the legislative jurisdiction of the constituent States or other similar territorial entities, the federal government shall refer the provisions to the authorities of those entities with a favourable endorsement, encouraging them to take appropriate action to give them effect.

Reservations (Article 42)

320. Article 42 provides for a number of reservation possibilities. This approach stems from the fact that the Convention covers an area of criminal law and criminal procedural law which is relatively new to many States. In addition, the global nature of the Convention, which will be open to member and non-member States of the Council of Europe, makes having such reservation possibilities necessary. These reservation possibilities aim at enabling the largest number of States to become Parties to the Convention, while permitting such States to maintain certain approaches and concepts consistent with their domestic law. At the same time, the drafters endeavoured to restrict the possibilities for making reservations so as to ensure that the largest possible extent the uniform application of the Convention by the Parties. Thus, no other reservations may be made than those enumerated. In addition, reservations may only be made by a Party at the time of signature or upon deposit of its instrument of ratification, acceptance, approval or accession.

321. Recognising that for some Parties certain reservations were essential to avoid conflict with their constitutional or fundamental legal principles, Article 43 imposes no specific time limit for the withdrawal of reservations. Instead, they should be withdrawn as soon as circumstances so permit.

322. In order to maintain some pressure on the Parties and to make them at least consider withdrawing their reservations, the Convention authorises the Secretary General of the Council of Europe to periodically enquire about the prospects for withdrawal. This possibility of enquiry is current practice under several Council of Europe instruments. The Parties are thus given an opportunity to indicate whether they still need to maintain their reservations in respect of certain provisions and to withdraw, subsequently, those which no longer prove necessary. It is hoped that over time Parties will be able to remove as many of their reservations as possible so as promote the Convention’s uniform implementation. Amendments (Article 44)
323. Article 44 takes its precedent from the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141), where it was introduced as an innovation in respect of criminal law conventions elaborated within the framework of the Council of Europe. The amendment procedure is mostly thought to be for relatively minor changes of a procedural and technical character. The drafters considered that major changes to the Convention could be made in the form of additional protocols.

324. The Parties themselves can examine the need for amendments or protocols under the consultation procedure provided for in Article 46. The European Committee on Crime Problems (CDPC) will in this regard be kept periodically informed and required to take the necessary measures to assist the Parties in their efforts to amend or supplement the Convention.

325. In accordance with paragraph 5, any amendment adopted would come into force only when all Parties have informed the Secretary General of their acceptance. This requirement seeks to ensure that the Convention will evolve in a uniform manner.

326. Article 45, paragraph 1, provides that the European Committee on Crime Problems (CDPC) should be kept informed about the interpretation and application of the provisions of the Convention. Paragraph 2 imposes an obligation on the Parties to seek a peaceful settlement of any dispute concerning the interpretation or the application of the Convention. Any procedure for solving disputes should be agreed upon by the Parties concerned. Three possible mechanisms for dispute-resolution are suggested by this provision: the European Committee on Crime Problems (CDPC) itself, an arbitral tribunal or the International Court of Justice.

Consultations of the Parties (Article 46)

327. Article 46 creates a framework for the Parties to consult regarding implementation of the Convention, the effect of significant legal, policy or technological developments pertaining to the subject of computer- or computer-related crime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Convention. The consultations shall in particular examine issues that have arisen in the use and implementation of the Convention, including the effects of declarations and reservations made under Articles 40 and 42.

328. The procedure is flexible and it is left to the Parties to decide how and when to convene if they so wish. Such a procedure was believed necessary by the drafters of the Convention to ensure that all Parties to the Convention, including non-member States of the Council of Europe, could be involved – on an equal footing basis – in any follow-up mechanism, while preserving the competences of the European Committee on Crime Problems (CDPC). The latter shall not only be kept regularly informed of the consultations taking place among the Parties, but also facilitate those and take the necessary measures to assist the Parties in their efforts to supplement or amend the Convention. Given the needs of effective prevention and prosecution of cyber-crime and the associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, non-governmental and private sector organisations, may be useful to these consultations (see also paragraph 14).

329. Paragraph 3 provides for a review of the Convention's operation after 3 years of its entry into force, at which time appropriate amendments may be recommended. The CDPC shall conduct such review with the assistance of the Parties.

330. Paragraph 4 indicates that except where assumed by the Council of Europe it will be for the Parties themselves to finance any consultations carried out in accordance with paragraph 1 of Article 46. However, apart from the European Committee on Crime Problems (CDPC) the Council of Europe Secretariat shall assist the Parties in their efforts under the Convention.

98/560/EC: Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry

COUNCIL RECOMMENDATION of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 130 thereof,

Having regard to the Commission's proposal,

Having regard to the opinion of the European Parliament (1),

Having regard to the opinion of the Economic and Social Committee (2),

(1) Whereas the Commission adopted the Green Paper on the protection of minors and human dignity in audiovisual and information services on 16 October 1996 and the Council received it favourably at its meeting on 16 December 1996;

(2) Whereas the European Parliament (3), the Economic and Social Committee (4) and the Committee of the Regions (5) have all adopted opinions on the Green Paper;

(3) Whereas the conclusions of the consultation process were submitted by the Commission to the Council at its meeting of 30 June 1997 and unanimously welcomed;

(4) Whereas on 16 October 1996, the Commission adopted the communication on illegal and harmful content on the Internet; whereas on 17 February 1997 the Council and the representatives of the Governments of the Member States, meeting within the Council, adopted the resolution on illegal

and harmful content on the Internet (6); whereas on 24 April 1997 the European Parliament adopted an opinion on the Commission communication on illegal and harmful content on the Internet; whereas this work is continuing in a manner complementary to the present recommendation since it deals with all forms of illegal and harmful content specifically on the Internet;

(5) Whereas the present recommendation addresses, in particular, issues of protection of minors and of human dignity in relation to audiovisual and information services made available to the public, whatever the means of conveyance (such as broadcasting, proprietary on-line services or services on the Internet);

(6) Whereas, in order to promote the competitiveness of the audiovisual and information services industry and its adaptation to technological development and structural changes, the provision of information, the raising of awareness and the education of users are essential; whereas this is also a condition of the European citizen's full participation in the information society; whereas, therefore, in addition to measures to protect minors and to combat illegal content offensive to human dignity, legal and responsible use of information and communication services should be encouraged, through the exercise, inter alia, of parental control measures;

States concerning the pursuit of television broadcasting activities (7) and in particular Articles 22, 22a and 22b of Directive 89/552/EEC, lays down a full range of measures aimed at the protection of minors with regard to television broadcasting for the purposes of ensuring the free movement of television broadcasts; (8) Whereas the development of audiovisual and information services is of vital importance for Europe in view of their significant potential in the fields of education, access to information and culture, economic development and job creation; (9) Whereas full achievement of this potential requires the existence of a successful and innovative industry in the Community; whereas it is in the first instance incumbent on businesses to ensure and improve their competitiveness with the support of public authorities where appropriate; (10) Whereas the establishment of the climate of confidence needed to achieve the potential of the audiovisual and information services industry by removing obstacles to the development and full competitiveness of the said industry is promoted by the protection of certain important general interests, in particular the protection of minors and of human dignity; (11) Whereas the general competitiveness of the European audiovisual and information services industry will improve through the development of an environment that favours cooperation between the enterprises in the sector on matters concerning the protection of minors and human dignity; (12) Whereas the existence of certain technological conditions enables a high level of protection of the abovementioned important general interests, in particular the protection of minors and human dignity, and, consequently, the acceptance by all users of these services; (13) Whereas it is important therefore to encourage enterprises to develop a national self-regulatory framework through cooperation between them and the other parties concerned; whereas self-regulation could provide enterprises with the means to adapt themselves rapidly to the quickening technical progress and to market globalization; (14) Whereas the protection of general interests sought in this manner must be seen in the context of the fundamental principles of respect for privacy and freedom of expression, as enshrined in Articles 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and as recognised by Article P(2) of the Treaty on European Union and by the case-law of the Court of Justice as general principles of Community law; (15) Whereas any restriction of these rights and freedoms must be non-discriminatory, necessary to achieving the desired objective and strictly proportional with regard to the limitations it imposes; (16) Whereas the global nature of communications networks necessitates an international approach to the question of the protection of minors and human dignity in audiovisual and information services; whereas, in this context, the development of a common indicative framework at European level makes it possible both to promote European values and make a decisive contribution to the international debate; (17) Whereas it is vital to distinguish between questions relating to illegal content which is offensive to human dignity and those relating to content that is legal, but liable to harm minors by impairing their physical or moral development; whereas these two types of problem may require a different approach and different solutions; (18) Whereas the national laws in which Member States have laid down rules and principles on the protection of minors and human dignity reflect cultural diversity and national and local sensitivities; whereas, in this regard, particular attention must be paid to the application of the principle of subsidiarity; (19) Whereas, in view of the transnational nature of communications networks, the effectiveness of national measures would be strengthened, at Community level, by coordination of national initiatives, and of the bodies responsible for their implementation, in accordance with the respective responsibilities and functions of the parties concerned and by the development of cooperation and the sharing of good practices in relevant areas; (20) Whereas, as a supplementary measure, and with full respect for the relevant regulatory frameworks at national and Community level, greater self-regulation by operators should contribute to the rapid implementation of concrete solutions to the problems of the protection of minors and human dignity, while maintaining the flexibility needed to take account of the rapid development of audiovisual and information services; (21) Whereas the contribution of the Community, the aim of which will be to supplement Member States’ measures to protect minors and human dignity in audiovisual and information services, should be based on the maximum use of existing instruments; (22) Whereas there should be close coordination of the various relevant initiatives conducted in parallel with the follow-up to the Green Paper, particularly the work on the follow-up to the communication on ‘Illegal and Harmful Content on the Internet’, including the resolution adopted by the Council and the representatives of the Governments of the Member States meeting within the Council on 17 February 1997, the 1997 European Parliament resolution and the two working party reports submitted to the Council on 28 November 1996 and 27 June 1997, work carried out according to the provisions of Article 22b of Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (8) and the work on cooperation on justice and home affairs; (23) Whereas the implementation of this recommendation will be closely coordinated with that of any possible new measure resulting from the work on the follow-up to the Commission communication on illegal and harmful content on the Internet, I. HEREBY RECOMMENDS that the Member States foster a climate of confidence which will promote the development of the audiovisual and information services industry by: (1) promoting, as a supplement to the regulatory framework, the establishment on a voluntary basis of national frameworks for the protection of minors and human dignity in audiovisual and information services through: - the encouragement, in accordance with national traditions and practices, of the participation of relevant parties (such as users, consumers, businesses and public authorities) in the definition, implementation and evaluation of national measures in the fields covered by this recommendation, - the establishment of a national framework for self-regulation by operators of on-line services, taking into account the indicative principles and methodology described in the Annex, - cooperation at Community level in developing comparable assessment methodologies; (2) encouraging broadcasters in their jurisdiction to carry out research and to experiment, on a voluntary basis, with new means of protecting minors and informing viewers, as a supplement to the national and Community regulatory frameworks governing broadcasting; (3) taking effective measures, where appropriate and feasible, to reduce potential obstacles to the development of the on-line services industry by sustaining the fight against illegal content offensive to human dignity, through: - the handling of complaints and the transmission of the necessary information about alleged illegal content to the relevant authorities at national level, - transnational cooperation between the complaints-handling structures, in order to strengthen the effectiveness of national measures; (4) promoting, in order to encourage the take-up of technological developments and in addition to and consistent with existing legal and other measures regarding broadcasting services, and in close cooperation with the parties concerned:
- action to enable minors to make responsible use of on-line audiovisual and information services, notably by improving the level of awareness among parents, educators and teachers of the potential of the new services and of the means whereby they may be made safe for minors,
- action to facilitate, where appropriate and necessary, identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places.

II. RECOMMENDS that the industries and parties concerned:
(1) cooperate, in accordance with national traditions and practices, with the relevant authorities in setting up structures representing all the parties concerned at national level, in order inter alia to facilitate participation in coordination at European and international level in the fields covered by this recommendation;
(2) cooperate in the drawing up of codes of conduct for the protection of minors and human dignity applying to the provision of on-line services, inter alia to create an environment favourable to the development of new services, taking into account the principles and the methodology described in the Annex;
(3) develop and experiment, as regards broadcasting services, on a voluntary basis, with new means of protecting minors and informing viewers in order to encourage innovation while improving such protection;
(4) develop positive measures for the benefit of minors, including initiatives to facilitate their wider access to audiovisual and information services, while avoiding potentially harmful content;
(5) collaborate in the regular follow-up and evaluation of initiatives carried out at national level in application of this recommendation.

III. INVITES the Commission to:
(1) facilitate, where appropriate through existing Community financial instruments, the networking of the bodies responsible for the definition and implementation of national self-regulation frameworks and the sharing of experience and good practices, in particular in relation to innovative approaches, at Community level, between the Member States and parties concerned in the various fields covered by this recommendation;
(2) encourage cooperation and the sharing of experience and good practices between the self-regulation structures and complaint-handling structures, with a view to fostering a climate of confidence by combating the circulation of illegal content offensive to human dignity in on-line audiovisual and information services;
(3) promote, with the Member States, international cooperation in the various fields covered by this recommendation, particularly through the sharing of experience and good practices between operators and other concerned parties in the Community and their partners in other regions of the world;
(4) develop, in cooperation with the competent national authorities, a methodology for evaluating the measures taken in pursuance of this recommendation, with particular attention to the evaluation of the added value of the cooperation process at Community level, and present, two years after the adoption of this recommendation, an evaluation report on its effect to the European Parliament and the Council.


For the Council
The President
J. FARNLEITNER

(1) Opinion delivered on 13 May 1998 (not yet published in the Official Journal).

ANNEX
INDICATIVE GUIDELINES FOR THE IMPLEMENTATION, AT NATIONAL LEVEL, OF A SELF-REGULATION FRAMEWORK FOR THE PROTECTION OF MINORS AND HUMAN DIGNITY IN ON-LINE AUDIOVISUAL AND INFORMATION SERVICES

Objective
The purpose of these guidelines is to foster a climate of confidence in the on-line audiovisual and information services industry by ensuring broad consistency, at Community level, in the development, by the businesses and other parties concerned, of national self-regulation frameworks for the protection of minors and human dignity. The services covered by these guidelines are those provided at a distance, by electronic means. They do not include broadcasting services covered by Council Directive 89/552/EEC or radio broadcasting. The contents concerned are those which are made available to the public, rather than private correspondence.
This consistency will enhance the effectiveness of the self-regulation process and provide a basis for the necessary transnational cooperation between the parties concerned.
While taking into account the voluntary nature of the self-regulation process (the primary purpose of which is to supplement existing legislation) and respecting the differences in approach and varying sensitivities in the Member States of the Community, these guidelines relate to four key components of a national self-regulation framework:
- consultation and representativeness of the parties concerned,
- code(s) of conduct,
- national bodies facilitating cooperation at Community level,
- national evaluation of self-regulation frameworks.

1. CONSULTATION AND REPRESENTATIVENESS OF THE PARTIES CONCERNED
The objective is to ensure that the definition, implementation and evaluation of a national self-regulation framework benefits from the full participation of the parties concerned, such as the public authorities, the users, consumers and the businesses which are directly or indirectly involved in the audiovisual and on-line information services industries. The respective responsibilities and functions of the parties concerned, both public and private, should be set out clearly. The voluntary nature of self-regulation means that the acceptance and effectiveness of a national self-regulation framework depends on the extent to which the parties concerned actively cooperate in its definition, application and evaluation.
All the parties concerned should also help with longer-term tasks such as the development of common tools or concepts (for example, on labelling of content) or the planning of ancillary measures (for example, on information, awareness and education).

2. CODE(S) OF CONDUCT
2.1. General
The objective is the production, within the national self-regulation framework, of basic rules which are strictly proportionate to the aims pursued; these rules should be incorporated into a code (or codes) of conduct covering at least the categories set out at 2.2, to be adopted and implemented voluntarily by the operators (i.e. primarily the businesses concerned).
In drawing up these rules, the following should be taken into account:
- the diversity of services and functions performed by the various categories of operator (providers of network, access, service, content, etc.) and their respective responsibilities,
- the diversity of environments and applications in on-line services (open and closed networks, applications of varying levels of interactivity).
In view of the above, operators may need one or more codes of conduct.
Given such diversity, the proportionality of the rules drawn up should be assessed in the light of:

- the principles of freedom of expression, protection of privacy and free movement of services,
- the principle of technical and economic feasibility, given that the overall objective is to develop the information society in Europe.

2.2. The content of the code(s) of conduct

The code (or codes) of conduct should cover the following:

2.2.1. Protection of minors

Objective: to ensure that minors to make responsible use of on-line services and to avoid them gaining access, without the consent of their parents or teachers, to legal content which may impair their physical, mental or moral development. Besides coordinated measures to educate minors and to improve their awareness, this should cover the establishment of certain standards in the following fields:

(a) Information to users

Objective: within the framework of encouraging responsible use of networks, on-line service providers should inform users, where possible, of any risks from the content of certain on-line services and of such appropriate means of protection as are available.

The codes of conduct should address, for example, the issue of basic rules on the nature of the information to be made available to users, its timing and the form in which it is communicated. The most appropriate occasions should be chosen to communicate the information (sale of technical equipment, conclusion of contracts with user, web sites, etc.).

(b) Presentation of legal contents which may harm minors

Objective: where possible, legal content which may harm minors or affect their physical, mental or moral development should be presented in such a way as to provide users with basic information on its potentially harmful effect on minors.

The codes of conduct should therefore address, for example, the issue of basic rules for the businesses providing on-line services concerned and for users and suppliers of content; the rules should set out the conditions under which the supply and distribution of content likely to harm minors should be subject, where possible, to protection measures such as:
- a warning page, visual signal or sound signal,
- descriptive labelling and/or classification of contents,
- systems to check the age of users.

Priority should be given, in this regard, to protection systems applied at the presentation stage to legal content which is clearly likely to be harmful to minors, such as pornography or violence.

(c) Support for parental control

Objective: where possible, parents, teachers and others exercising control in this area should be assisted by easy-to-use and reliable tools in order to enable, without the former’s educational choices being compromised, minors under their charge to have access to services, even when unsupervised.

The codes of conduct should address, for example, the issue of basic rules on the conditions under which, wherever possible, additional tools or services are supplied to users to facilitate parental control, including:
- filter software installed and activated by the user,
- filter options activated, at the end-user’s request, by service operators at a higher level (for example, limiting access to predefined sites or offering general access to services).

(d) Handling of complaints (‘hotlines’)

Objective: to promote the effective management of complaints about content which does not comply with the rules on the protection of minors and/or violates the code of conduct.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints, etc.).

2.2.2. Protection of human dignity

Objective: to support effective measures in the fight against illegal content offensive to human dignity.

(a) Information for users

Objective: where possible, users should be clearly informed of the risks inherent in the use of on-line services as content providers so as to encourage legal and responsible use of networks.

Codes of conduct should address, for example, the issue of basic rules on the nature of information to be made available, its timing and the form in which it is to be communicated.

(b) Handling of complaints (‘hotlines’)

Objective: to promote the effective handling of complaints about illegal content offensive to human dignity circulating in audiovisual and on-line services, in accordance with the respective responsibilities and functions of the parties concerned, so as to reduce illegal content and misuse of the networks.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints, etc.).

(c) Cooperation of operators with judicial and police authorities

Objective: to ensure, in accordance with the responsibilities and functions of the parties concerned effective cooperation between operators and the judicial and police authorities within Member States in combating the production and circulation of illegal content offensive to human dignity in audiovisual and on-line information services.

The codes of conduct should address, for example, the issue of basic rules on cooperation procedures between operators and the competent public authorities, while respecting the principles of proportionality and freedom of expression as well as relevant national legal provisions.

2.2.3. Violations of the codes of conduct

Objective: to strengthen the credibility of the code (or codes) of conduct, taking account of its voluntary nature, by providing for dissuasive measures which are proportionate to the nature of the violations. In this connection, provision should be made, where appropriate, for appeal and mediation procedures.

Appropriate rules to govern this area should be included in the code of conduct.

3. NATIONAL BODIES FACILITATING COOPERATION AT COMMUNITY LEVEL

Objective: to facilitate cooperation at Community level (sharing of experience and good practices; working together) through the networking of the appropriate structures within Member States, consistent with their national functions and responsibilities. Such structures could also allow international cooperation to be extended.

Cooperation at European level means:
- cooperation between the parties concerned:
  - all the parties involved in the drawing up of the national self-regulation framework are asked to set up a representative body at national level to facilitate the sharing of experience and good practices and to work together at Community and international level.
- cooperation between national complaints-handling structures:
  - to facilitate and develop cooperation at European and international level, the parties involved in an effective complaint management system are asked to set up a national contact point to strengthen cooperation in the fight against illegal content, facilitate the sharing of experience and good practices, and improve legal and responsible use of the networks.

4. EVALUATION OF SELF-REGULATION FRAMEWORKS

The objective is to provide for regular evaluations of the self-regulation framework at national level, to assess its...
effectiveness in protecting the general interests in question, to measure its success in achieving its objectives and to adapt it gradually to changes in the market, technology and types of use. The parties concerned are asked to set up an evaluation system at national level so that they can monitor the progress made in implementing the self-regulation framework. This should take into account appropriate European-level cooperation, inter alia on the development of comparable assessment methodologies.


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee(1),

After consulting the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(2),

Whereas:
(1) Communication networks and information systems have become an essential factor in economic and societal development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply already are. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society not least because of the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks, that may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens.

(2) The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to the development of e-commerce. Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. Member States have taken several supporting measures, such as information campaigns and research projects, to enhance network and information security throughout society.

(3) The technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public actors that bear their own responsibility risk undermining the smooth functioning of the Internal Market.

(4) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (the Framework Directive)(3) lays down the tasks of national regulatory authorities, which include cooperating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to ensuring a high level of protection of personal data and privacy, and ensuring that the integrity and security of public communications networks are ensured.


(6) Directive 2002/20/EC entitles Member States to attach to the general authorisation, conditions regarding the security of public networks against unauthorised access in accordance with Directive 97/66/EC(11).

(7) Directive 2002/22/EC requires that Member States take necessary steps to ensure the integrity and availability of the public telephone networks at fixed locations and that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

(8) Directive 2002/58/EC requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard security of its services and also requires the confidentiality of the communications and related traffic data. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(12), requires Member States to provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing.

(9) Directive 2002/21/EC and Directive 1999/93/EC contain provisions on standards that are to be published in the Official Journal of the European Union. Member States also use standards from international bodies as well as de facto standards developed by the global industry. It is necessary for the Commission and the Member States to be able to track those standards which meet the requirements of Community legislation.

(10) These internal market measures require different forms of technical and organisational applications by the Member States and the Commission. These are technically complex tasks with no single, self-evident solutions. The heterogeneous application of these requirements can lead to inefficient solutions and create obstacles to the internal market. This calls for the creation of a centre of expertise at European level providing guidance, advice, and when called upon, with assistance within its objectives, which may be relied upon by the European Parliament, the Commission or competent bodies appointed by the Member States. National Regulatory Authorities, designated under Directive 2002/21/EC, can be appointed by a Member State as a competent body.

(11) The establishment of a European agency, the European Network and Information Security Agency, hereinafter referred to as "the Agency", operating as a point of reference and establishing confidence by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it, would respond to these needs. The Agency should build on national and Community efforts and therefore perform its
tasks in full cooperation with the Member States and be open to contacts with industry and other relevant stakeholders. As electronic networks, to a large extent, are privately owned, the Agency should build on the input from and cooperation with the private sector.

(17) The exercise of the Agency’s tasks should not interfere with the competences and should not pre-empt, impede or overlap with the relevant powers and tasks conferred on:
- the national regulatory authorities as set out in the Directives relating to the electronic communications networks and services on the European level and Services established by Commission Decision 2002/627/EC and the Communications Committee referred to in Directive 2002/21/EC.
- the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services (14),
- the supervisory authorities of the Member States relating to the protection of individuals with the regard to the processing of personal data and on the free movement of such data.

(13) To understand better the challenges in the network and information security field, there is a need for the Agency to analyse current and emerging risks and for that purpose the Agency may collect appropriate information, in particular through questionnaires, without imposing new obligations on the private sector or the Member States to generate data. Emerging risks should be understood as issues already visible as possible future risks to network and information security.

(14) Ensuring confidence in networks and information systems requires that individuals, businesses and public administrations are sufficiently informed, educated and trained in the field of network and information security. Public authorities have a role in increasing awareness by informing the general public, small and medium-sized enterprises, corporate companies, public administrations, schools and universities. These measures need to be further developed. An increased information exchange between Member States will facilitate such awareness raising actions. The Agency should provide advice on best practices in awareness-raising, training and courses.

(15) The Agency should have the task of contributing to a high level of network and information security within the Community and of developing a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union, thus contributing to the systemic development of the internal market.

(16) Efficient security policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods and procedures are used at different levels with no common practice on their efficient application. The promotion and development of best practices for risk assessment and for interoperable risk management solutions within public and private sector organisations will increase the security level of networks and information systems in Europe.

(17) The work of the Agency should utilise ongoing research, development and technological assessment activities, in particular those carried out by the different Community research initiatives.

(18) Where appropriate and useful for fulfilling its scope, objectives and tasks, the Agency could share experience and general information with bodies and agencies created under European Union law and dealing with network and information security.

(19) Network and information security problems are global issues. There is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security. Efficient cooperation with third countries and the global community has become a task also at European level. To this end, the Agency should contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations.

(20) In its activities the Agency should pay attention to small and medium-sized enterprises.

(21) In order effectively to ensure the accomplishment of the tasks of the Agency, the Member States and the Commission should be represented on the Executive Board, with the necessary powers to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, approve the Agency’s work programme, adopt its own rules of procedure and the Agency’s internal rules of operation, appoint and remove the Executive Director. The Management Board should ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with this Regulation.

(22) A Permanent Stakeholders’ Group would be helpful, in order to maintain a regular dialogue with the private sector, consumers organisations and other relevant stakeholders. The Permanent Stakeholders’ Group, established and chaired by the Executive Director, should focus on issues relevant to all stakeholders and bring them to the attention of the Executive Director. The Executive Director may, where appropriate and according to the agency’s working programme, invite representatives of the European Parliament and from other relevant bodies to take part in the meetings of the Group.

(23) The smooth functioning of the Agency requires that its Executive Director is appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security and that he/she performs his/her duties with complete independence and flexibility as to the organisation of the internal functioning of the Agency. To this end, the Executive Director should be appointed by the Commission and of the Permanent Stakeholders’ Group, and take all necessary steps to ensure the proper accomplishment of the work of the Agency. The Agency should prepare each year a draft general report to be submitted to the Management Board, should draw up a draft statement of estimates of revenue and expenditure of the Agency and should implement the budget.

(24) The Executive Director should have the possibility to set up ad hoc Working Groups to address in particular scientific and technical matters. In establishing the ad hoc Working Groups the Executive Director should seek input from and mobilise the relevant expertise of the private sector. The ad hoc Working Groups should enable the Agency to have access to the most updated information available in order to be able to respond to the security challenges posed by the developing information society. The Agency should ensure that its ad hoc Working Groups are competent and representative and that they include, as appropriate according to the specific issues, representation of the public administrations of the Member States, of the private sector including industry, of the users and of academic experts in network and information security. The Agency may, if necessary, add to the Working Groups independent experts recognised as competent in the field concerned. The experts who participate in the ad hoc Working Groups organised by the Agency should not belong to the Agency’s staff. Their expenses should be met by the Agency in accordance with its internal rules and in conformity with the existing Financial Regulations.

26. Within its scope, its objectives and in the performance of its tasks, the Agency should comply in particular with the provisions applicable to the Community institutions, as well as the national legislation regarding the treatment of sensitive documents.

27. In order to guarantee the full autonomy and independence of the Agency, it is considered necessary to grant it an autonomous budget whose revenue comes essentially from a contribution from the Community. The Community budgetary procedure remains applicable as far as any subsidies chargeable to the general budget of the European Union are concerned. Moreover, the Court of Auditors should undertake the auditing of accounts.

28. Where necessary and on the basis of arrangements to be concluded, the Agency may have access to the interpretation services provided by the Directorate General for Interpretation (DGI) of the Commission, or by Interpretation Services of other Community institutions.

29. The Agency should be initially established for a limited period and its operations evaluated in order to determine whether the duration of its operations should be extended, HAVE ADOPTED THIS REGULATION:

SECTION 1 SCOPE, OBJECTIVES AND TASKS

Article 1 Scope
1. For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security, thereby ensuring the smooth functioning of the internal market, a European Network and Information Security Agency is hereby established, hereinafter referred to as “the Agency”. The Agency shall develop a high level of expertise. The Agency shall use its services provided by the Directorate General for Internal Market and Services of other Community institutions.

2. The Agency shall provide assistance and deliver advice to the Member States and, as a consequence, the business community to contribute to the smooth functioning of the internal market, including those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

3. The objectives and the tasks of the Agency shall be without prejudice to the competencies of the Member States concerning network and information security which fall outside the scope of the EC Treaty, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law.

Article 2 Objectives
1. The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.

2. The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this Regulation.

3. Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use its services and offer its assistance within its objectives.

4. The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

Article 3 Tasks
1. In order to ensure that the scope and objectives set out in Articles 1 and 2 are complied with and met, the Agency shall perform the following tasks:

(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;

(b) provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member States with advice, and when called upon, with assistance within its objectives;

(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;

(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;

(e) contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives;

(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;

(g) track the development of standards for products and services on network and information security;

(h) advise the Commission on research in the area of network and information security and whenever possible in the area of prevention technologies;

(i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;

(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;

(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

Article 4 Definitions
For the purposes of this Regulation the following definitions shall apply:

(a) “network” means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed;

(b) “information system” means computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(c) “network and information security” means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;

(d) “availability” means that data is accessible and services are operational;
(e) “authentication” means the confirmation of an asserted identity of entities or users;  
(f) “data integrity” means the confirmation that data which has been sent, received, or stored are complete and unchanged;  
(g) “data confidentiality” means the protection of communications or stored data against interception and reading by unauthorised persons;  
(h) “risk” means a function of the probability that a vulnerability in the system affects authentication or the availability, authenticity, integrity or confidentiality of the data processed or transferred and the severity of that effect, consequential to the intentional or non-intentional use of such a vulnerability;  
(i) “risk assessment” means a scientific and technologically based process consisting of four steps, threats identification, threat characterisation, exposure assessment and risk characterisation;  
(j) “risk management” means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options;  
(k) “culture of network and information security” has the same meaning as that set out in the OECD Guidelines for the security of Information Systems and Networks of 25 July 2002 and the Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security [17].

SECTION 2 ORGANISATION

Article 5

Bodies of the Agency

The Agency shall comprise:  
(a) a Management Board;  
(b) an Executive Director, and  
(c) a Permanent Stakeholders’ Group.

Article 6

Management Board

1. The Management Board shall be composed of one representative of each Member State, three representatives appointed by the Commission, as well as three representatives, proposed by the Commission and appointed by the Council, without the right to vote, each of whom represents one of the following groups:

(a) information and communication technologies industry;  
(b) consumer groups;  
(c) academic experts in network and information security.

2. Board members shall be appointed on the basis of their degree of relevant experience and competence in the field of network and information security. Representatives may be replaced by alternates, appointed at the same time.

3. The Management Board shall elect its Chairperson and a Deputy Chairperson from among its members for a two-and-a-half-year period, which shall be renewable. The Deputy Chairperson shall ex-officio replace the Chairperson in the event of the Chairperson being unable to attend to his/her duties.

4. The Management Board shall adopt its rules of procedure, on the basis of a proposal by the Commission. Unless otherwise provided, the Management Board shall take its decisions by a majority of its members with the right to vote. A two-thirds majority of all members with the right to vote is required for the adoption of its rules of procedure, the Agency’s internal rules of operation, the budget, the annual work programme, as well as the appointment and the removal of the Executive Director.

5. Meetings of the Management Board shall be convened by its Chairperson. The Management Board shall hold an ordinary meeting twice a year. It shall also hold extraordinary meetings at the instance of the Chairperson or at the request of at least a third of its members with the right to vote. The Executive Director shall take part in the meetings of the Management Board, without voting rights, and shall provide the Secretariat.

6. The Management Board shall adopt the Agency’s internal rules of operation on the basis of a proposal by the Commission. These rules shall be made public.

7. The Management Board shall define the general orientations for the operation of the Agency. The Management Board shall ensure that the Agency works in accordance with the principles laid down in Articles 12 to 14 and 23. It shall also ensure consistency of the Agency’s work with activities conducted by Member States as well as at Community level.

8. Before 30 November each year, the Management Board, having received the Commission’s opinion shall adopt the Agency’s work programme for the following year. The Management Board shall ensure that the work programme is consistent with the Agency’s scope, objectives and tasks as well as with the Community’s legislative and policy priorities in the area of network and information security.

9. Before 31 March each year, the Management Board shall adopt the general report on the Agency’s activities for the previous year.

10. The financial rules applicable to the Agency shall be adopted by the Management Board after the Commission has been consulted. They may not depart from Commission Regulation (EC, Euratom) No 2343/2002 of 19 November 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of the Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities [18], unless such departure is specifically required for the Agency’s operation and the Commission has given its prior consent.

Article 7

Executive Director

1. The Agency shall be managed by its Executive Director, who shall be independent in the performance of his/her duties.

2. The Executive Director shall be appointed by the Management Board on the basis of a list of candidates proposed by the Commission after an open competition following publication in the Official Journal of the European Union and elsewhere of a call for expressions of interest. The Executive Director shall be appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security. Before appointment the candidate nominated by the Management Board shall be invited without delay to make a statement before the European Parliament and to answer questions put by members of that institution. The European Parliament or the Council may also ask at any time for a hearing with the Executive Director on any subject related to the Agency’s activities. The Executive Director may be removed from office by the Management Board.

3. The term of office of the Executive Director shall be up to five years.

4. The Executive Director shall be responsible for:

(a) the day-to-day administration of the Agency;  
(b) drawing up a proposal for the Agency’s work programmes after prior consultation of the Commission and of the Permanent Stakeholders’ Group;  
(c) implementing the work programmes and the decisions adopted by the Management Board;  
(d) ensuring that the Agency carries out its tasks in accordance with the requirements of those using its services, in particular with regard to the adequacy of the services provided;  
(e) the preparation of the Agency’s draft statement of estimates of revenue and expenditure and the execution of its budget;  
(f) all staff matters;  
(g) developing and maintaining contact with the European Parliament and for ensuring a regular dialogue with its relevant committees;  
(h) developing and maintaining contact with the business community and consumers organisations for ensuring a regular dialogue with relevant stakeholders;  
(i) chairing the Permanent Stakeholders’ Group.
5. Each year, the Executive Director shall submit to the Management Board for approval:
(a) a draft general report covering all the activities of the Agency in the previous year;
(b) a draft work programme.
6. The Executive Director shall, following adoption by the Management Board, forward the work programme to the European Parliament, the Council, the Commission and the Member States and shall have it published.
7. The Executive Director shall, following adoption by the Management Board, transmit the Agency's general report and the European Parliament, the Council, the Commission, the Court of Auditors, the European Economic and Social Committee and the Committee of the Regions and shall have it published.
8. Where necessary and within the Agency's scope, objectives and tasks, the Executive Director may establish, in consultation with the Permanent Stakeholders' Group, ad hoc Working Groups composed of experts. The Management Board shall be duly informed. The procedures regarding in particular the composition, the appointment of the experts by the Executive Director and the operation of the ad hoc Working Groups shall be specified in the Agency's internal rules of operation.

Where established, the ad hoc Working Groups shall address in particular technical and scientific matters.

Members of the Management Board may not be members of the ad hoc Working Groups. Representatives of the Commission shall be entitled to be present in their meetings.

Article 8
Permanent Stakeholders' Group
1. The Executive Director shall establish a Permanent Stakeholders' Group composed of experts representing the relevant stakeholders, such as information and communication technologies industry, consumer groups and academic experts in network and information security.
2. The procedures regarding in particular the number, the composition, the appointment of the members by the Executive Director and the operation of the Group shall be specified in the Agency's internal rules of operation and shall be made public.
3. The Group shall be chaired by the Executive Director. The term of office of its members shall be two-and-a-half years. Members of the Group may not be members of the Management Board.
4. Representatives of the Commission shall be entitled to be present in the meetings.
5. The Group may advise the Executive Director in the performance of his/her duties under this Regulation, in drawing up a proposal for the Agency's work programme, as well as in ensuring communication with the relevant stakeholders on all issues related to the work programme.

SECTION 3 OPERATION
Article 9
Work programme
The Agency shall base its operations on carrying out the work programme adopted in accordance with Article 6(8). The work programme shall not prevent the Agency from taking up unforeseen activities that fall within its scope and objectives and within the given budget limitations.

Article 10
Requests to the Agency
1. Requests for advice and assistance falling within the Agency's scope, objectives and tasks shall be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. The Executive Director shall inform the Commission of the received requests. If the Agency refuses a request, justification shall be given.
2. Requests referred to in paragraph 1 may be made by:
(a) the European Parliament;
(b) the Commission;
(c) any competent body appointed by a Member State, such as a national regulatory authority as defined in Article 2 of Directive 2002/21/EC.
3. The practical arrangements for the application of paragraphs 1 and 2, regarding in particular the submission, the prioritisation, the follow up as well as the information of the Management Board on the requests to the Agency shall be laid down by the Management Board in the Agency's internal rules of operation.

Article 11
Declaration of interests
1. The Executive Director, as well as officials seconded by Member States on a temporary basis shall make a declaration of commitments and a declaration of interests indicating the absence of any direct or indirect interests, which might be considered prejudicial to their independence. Such declarations shall be made public.
2. External experts participating in ad hoc Working Groups, shall declare at each meeting any interests, which might be considered prejudicial to their independence in relation to the items on the agenda.

Article 12
Transparency
1. The Agency shall ensure that it carries out its activities with a high level of transparency and in accordance with Article 13 and 14.
2. The Agency shall ensure that the public and any interested parties are given objective, reliable and easily accessible information, in particular with regard to the results of its work, where appropriate. It shall also make public the declarations of interest made by the Executive Director and by officials seconded by Member States on a temporary basis, as well as the declarations of interest made by experts in relation to items on the agenda of meetings of the ad hoc Working Groups.
3. The Management Board, acting on a proposal from the Executive Director, may authorize interested parties to observe the proceedings of some of the Agency's activities.

Article 13
Confidentiality
1. Without prejudice to Article 14, the Agency shall not divulge to third parties information that it processes or receives for which confidential treatment has been requested.
2. Members of the Management Board, the Executive Director, the members of the Permanent Stakeholders Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis, even after their duties have ceased, are subject to the requirements of confidentiality pursuant to Article 287 of the Treaty.
3. The Agency shall lay down in its internal rules of operation the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 14
Access to documents
1. Regulation (EC) No 1049/2001 shall apply to documents held by the Agency.
2. The Management Board shall adopt arrangements for implementing the Regulation (EC) No 1049/2001 within six months of the establishment of the Agency.
3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may form the subject of a complaint to the Ombudsman or of an action before the Court of Justice of the European Communities, under Articles 195 and 230 of the Treaty respectively.

SECTION 4 FINANCIAL PROVISIONS
Article 15
Adoption of the budget
1. The revenues of the Agency shall consist of a contribution from the Community and any contribution from third
countries participating in the work of the Agency as provided for by Article 24.

2. The expenditure of the Agency shall include the staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts entered into with third parties.

3. By 1 March each year at the latest, the Executive Director shall draw up a draft statement of estimates of the Agency’s revenue and expenditure for the following financial year, and shall forward it to the Management Board, together with a draft establishment plan.

4. Revenue and expenditure shall be in balance.

5. Each year, the Management Board, on the basis of a draft statement of estimates of revenue and expenditure drawn up by the Executive Director, shall produce a statement of estimates of revenue and expenditure for the Agency for the following financial year.

6. This statement of estimates, which shall include a draft establishment plan together with the provisional work programme, shall by 31 March at the latest, be transmitted by the Management Board to the Commission and the States with which the Community has concluded agreements in accordance with Article 24.

7. This statement of estimates shall be forwarded by the Commission to the European Parliament and the Council (both hereinafter referred to as the “budgetary authority”) together with the preliminary draft general budget of the European Union.

8. On the basis of this statement of estimates, the Commission shall enter in the preliminary draft general budget of the European Union the estimates it deems necessary for the establishment plan and the amount of the subsidy to be charged to the general budget, which it shall submit to the budgetary authority in accordance with Article 272 of the Treaty.

9. The budgetary authority shall authorise the appropriations for the subsidy to the Agency.

10. The Management Board shall adopt the establishment plan for the Agency.

11. The Management Board shall adopt the Agency’s budget. It shall become final following final adoption of the general budget of the European Union. Where appropriate, the Agency’s budget shall be adjusted accordingly. The Management Board shall forward it without delay to the Commission and the budgetary authority.

12. The Management Board shall, as soon as possible, notify the budgetary authority of its intention to implement any project which may have significant financial implications for the Agency in respect of its own staff.

13. The staff of the Agency, including its Executive Director, shall be subject to the rules and regulations applicable to the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF) (20) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

14. The implementation of the budget shall be subject to monitoring by the authorities authorised to conclude contracts by the Conditions of Employment of Other Servants, shall be exercised by the Agency in respect of its own staff.

15. The Agency may also employ officials seconded by Member States on a temporary basis and for a maximum of five years.

16. The Executive Director shall implement the Agency’s budget.

17. The powers conferred on the budgetary authority authorised to conclude contracts by the Conditions of Employment of Other Servants, shall be exercised by the Agency in respect of its own staff.

18. The Agency may also employ officials seconded by Member States on a temporary basis and for a maximum of five years.

19. The Protocol on the Privileges and Immunities of the European Communities shall apply to the Agency and its staff.
Liability

1. The contractual liability of the Agency shall be governed by the law applicable to the contract in question.

The Court of Justice of the European Communities shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.

2. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by it or its servants in the performance of their duties.

The Court of Justice shall have jurisdiction in any dispute relating to compensation for such damage.

3. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Article 22

Languages

1. The provisions laid down in Regulation No 1 of 15 April 1958 determining the languages to be used in the European Economic Community(22) shall apply to the Agency. The Member States and the other bodies appointed by them may address the Agency and receive a reply in the Community language of their choice.

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union(23).

Article 23

Protection of personal data

When processing data relating to individuals, the Agency shall be subject to the provisions of Regulation (EC) No 45/2001.

Article 24

Participation of third countries

1. The Agency shall be open to the participation of countries, which have concluded agreements with the European Community by virtue of which they have adopted and applied Community legislation in the field covered by this Regulation.

2. Arrangements shall be made under the relevant provisions of those agreements, specifying in particular the nature, extent and manner in which these countries will participate in the Agency’s work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff.

SECTION 6 FINAL PROVISIONS

Article 25

Review clause

1. By 17 March 2007, the Commission, taking into account the views of all relevant stakeholders, shall carry out an evaluation on the basis of the terms of reference agreed with the Management Board. The Commission shall undertake the evaluation, notably with the aim to determine whether the duration of the Agency should be extended beyond the period specified in Article 27.

2. The evaluation shall assess the impact of the Agency on the policies and practices and envisage, if necessary, the appropriate changes to this Regulation to the benefit of those affected.

Article 26

Administrative control

The operations of the Agency are subject to the supervision of the Ombudsman in accordance with the provisions of Article 195 of the Treaty.

Article 27

Duration

The Agency shall be established from 14 March 2004 for a period of five years.

Article 28

Entry into force

This Regulation shall enter into force on the day following that of its publication in the Official Journal of the European Union. This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Strasbourg, 10 March 2004.

The President

P. Cox

For the Council

The President

D. Roche


Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31(1)(e) and 34(2)(b) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Whereas:

(1) The objective of this Framework Decision is to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

(2) There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.


(4) The need to further increase awareness of the problems related to information security and provide practical assistance has also been stressed in the European Parliament Resolution of 5 September 2001.

(5) Significant gaps and differences in Member States' laws in this area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in the area of attacks against information systems. The transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

(6) The Action Plan of the Council and the Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice [3], the Tampere European Council on 15 to 16 October 1999, the Santa Maria da Feira European Council on 19 to 20 June 2000, the Commission in the "Scoreboard" and the European Parliament in its Resolution of 19 May 2000 indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.

(7) It is necessary to complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8's work on transnational cooperation in the area of high tech crime, by providing a common approach in the European Union in this area. This call was further elaborated by the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

(8) Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.

(9) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The personal data processed in the context of the implementation of this Framework Decision should be protected in accordance with the principles of the said Convention.

(10) Common definitions in this area, particularly of information systems and computer data, are important to ensure a consistent approach in Member States in the application of this Framework Decision.

(11) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for common offences of illegal access to an information system, illegal system interference and illegal data interference.

(12) In the interest of combating computer-related crime, each Member State should ensure effective judicial cooperation in respect of offences based on the types of conduct referred to in Articles 2, 3, 4 and 5.

(13) There is a need to avoid over-criminalisation, particularly of minor cases, as well as a need to avoid criminalising right-holders and authorised persons.

(14) There is a need for Member States to provide for penalties for attacks against information systems. The penalties thus provided for shall be effective, proportionate and dissuasive.

(15) It is appropriate to provide for more severe penalties when an attack against an information system is committed within the framework of a criminal organisation, as defined in the Joint Action 98/733 JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member State of the European Union [4]. It is also appropriate to provide for more severe penalties where such an attack has caused serious damages or has affected essential interests.

(16) Measures should also be foreseen for the purposes of cooperation between Member States with a view to ensuring effective action against attacks against information systems. Member States should therefore make use of the existing network of operational contact points referred to in the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime [5], for the exchange of information.

(17) Since the objectives of this Framework Decision, ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, as rules have to be common and compatible, and can therefore be better achieved at the level of the Union, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in that Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.
Article 1
Definitions
For the purposes of this Framework Decision, the following definitions shall apply:
(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;
(b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;
(c) "legal person" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations;
(d) "without right" means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation.

Article 2
Illegal access to information systems
1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.
2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

Article 3
Illegal system interference
1. Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4
Illegal data interference
Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 5
Instigation, aiding and abetting and attempt
1. Each Member State shall ensure that the instigation of aiding and abetting an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence.
2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence.
3. Each Member State may decide not to apply paragraph 2 for the offences referred to in Article 2.

Article 6
Penalties
1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 2, 3, 4 and 5 are punishable by effective, proportionate and dissuasive criminal penalties.
2. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between one and three years of imprisonment.

Aggravating circumstances
1. Each Member State shall take the necessary measures to ensure that the offence referred to in Article 2(2) and the offence referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between two and five years of imprisonment when committed within the framework of a criminal organisation as defined in Joint Action 98/733/JHA apart from the penalty level referred to therein.
2. A Member State may also take the measures referred to in paragraph 1 when the offence has caused serious damages or has affected essential interests.

Article 8
Liability of legal persons
1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:
(a) a power of representation of the legal person, or
(b) an authority to make decisions on behalf of the legal person, or
(c) an authority to exercise control within the legal person.
2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person may be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority.
3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of the offences referred to in Articles 2, 3, 4 and 5.

Article 9
Penalties for legal persons
1. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other penalties, such as:
(a) exclusion from entitlement to public benefits or aid;
(b) temporary or permanent disqualification from the practice of commercial activities;
(c) placing under judicial supervision; or
(d) a judicial winding-up order.
2. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(2) is punishable by effective, proportionate and dissuasive penalties or measures.

Article 10
Jurisdiction
1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 2, 3, 4 and 5 where the offence has been committed:
(a) in whole or in part within its territory; or
(b) by one of its nationals; or
(c) for the benefit of a legal person that has its head office in the territory of that Member State.
2. When establishing its jurisdiction in accordance with paragraph 1(a), each Member State shall ensure that the jurisdiction includes cases where:
(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or
(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.
3. A Member State which, under its law, does not as yet extradite or surrender its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, the offences referred to in
Articles 2, 3, 4 and 5, when committed by one of its nationals outside its territory.
4. Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors:
- the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2,
- the Member State shall be that of which the perpetrator is a national,
- the Member State shall be that in which the perpetrator has been found.
5. A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c).
6. Member States shall inform the General Secretariat of the Council and the Commission where they decide to apply paragraph 5, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

Article 11
Exchange of information
1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week.
2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall forward that information to the other Member States.

Article 12
Implementation
1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision by 16 March 2007.
2. By 16 March 2007 Member States shall transmit to the General Secretariat of the Council and to the Commission the text of any provisions transposing into their national law the obligations imposed on them under this Framework Decision. By 16 September 2007, on the basis of a report established on the basis of information and a written report by the Commission, the Council shall assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 13
Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union. Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.

Entry into force
This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.
Done at Brussels, 24 February 2005.

For the Council
The President
N. Schmit

The President
Council

Done at Brussels, 24 February 2005.
 Somebody
the electronic communications sector (Directive on privacy and electronic communications) requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard the security of its services.

24 Those obligations should also be extended to public administrations and market operators which perform the maintenance of their network and information systems managed either by their internal IT staff or the systems managed by their external service providers. These obligations should include the implementation of the notification obligations, competent authorities should pay due attention to the relevant market operators and public administrations regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

25 To avoid imposing a disproportionate financial and administrative burden on small operators and users, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures. These requirements should not apply to micro enterprises.

26 Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators and public administrations in order to assess the level of security of network and information systems as well as reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems. Criminal activities are in many cases underlying an incident. The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.

27 Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. Member states shall implement the obligations of notifying incidents in a way that minimises the administrative burden in case the security incident is also a personal data breach in line with the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal data, thereby easing the administrative burden on businesses and public administrations.


29 The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions.

30 In order to allow for the proper functioning of the cooperation network, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, of the further specification of the triggering events for early warning, and of the definition of the circumstances in which market operators and public administrations are required to notify incidents.

31 It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

32 In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be exercisable in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Software developers and hardware manufacturers are not providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.

33 Technical and organisational measures imposed to public administrations and market operators should ensure security of the networks and systems which are under their control. These should be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. The security and notification obligations should apply to the relevant market operators and public administrations regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

34 Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Software developers and hardware manufacturers are not providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.
(37) In the application of this Directive, the Commission shall liaise as appropriate with relevant sectoral committees and relevant bodies set up at EU level in particular in the field of energy, transport and health.

(38) Information that is considered confidential by a competent authority, in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission and other competent authorities only where such exchange is strictly necessary for the application of this Directive. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such exchange.

(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the national competent authorities may require the processing of personal data. Such processing of personal data is necessary to meet the objectives of public interest pursued by this Directive and is thus legitimate under Article 7 of Directive 95/46/EC. It does not constitute, in relation to these legitimate aims, a disproportionate and intolerable interference impairing the very substance of the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate. Where data are processed by Union institutions and bodies, such processing for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

(40) Since the objectives of this Directive, namely to ensure a high level of NIS in the Union, cannot be sufficiently achieved by the Member States alone and can therefore, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(41) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union notably, the right to respect for private life and communications, the protection for personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles.

H ave a do ted th is Di rect iv e: 

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter and scope

This Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union. To that end, this Directive:

(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;

(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting networks and information systems;

(c) establishes security requirements for market operators and public administrations.

The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to service providers. This Directive shall be without prejudice to EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.


The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.

Article 2 Minimum harmonisation

Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under Union law.

Article 3 Definitions

For the purpose of this Directive, the following definitions shall apply:

(1) "network and information system" means:

(a) an electronic communications network within the meaning of Directive 2002/21/EC, and

(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as

(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.

(2) "security" means the ability of a network and information system to resist, at a given level of confidence, accidental or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;

(3) "risk" means any circumstance or event having a potential adverse effect on security;

(4) "incident" means any circumstance or event having an actual adverse effect on security;

(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;

(6) "NIS cooperation plan" means a plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of a risk or an incident affecting them;

(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;

(8) "market operator" means any of the following providers of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II:

(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;

(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.

(9) "standard" means a standard referred to in Regulation (EU) No 1025/2012;

(10) "specification" means a specification referred to in Regulation (EU) No 1025/2012;
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.

Article 4
National NIS strategy and national NIS cooperation plan
1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security. The national NIS strategy shall address in particular the following issues:
   (a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis;
   (b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant sectors;
   (c) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;
   (d) An indication of the education, awareness raising and training programmes;
   (e) Research and development plans and a description of how these plans reflect the identified priorities.
2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements
   (a) A risk assessment plan to identify risks and assess the impacts of potential incidents;
   (b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;
   (c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;
   (d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.

Article 6
National competent authority on the security of network and information systems
Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority"). The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.
Member States shall ensure that the competent authorities have adequate technical, financial and human resources to carry out an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the competent authorities via the network referred to in Article 8.
Member States shall ensure that the competent authorities receive the notifications of incidents from public administrations and market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.

The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities. Each Member State shall notify to the Commission without delay the designation of the competent authority, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority.

Article 7
Computer Emergency Response Team
Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.
Member States shall ensure that CERTs have adequate technical, financial and human resources to effectively carry out their tasks set out in point (2) of Annex I.
Member States shall ensure that CERTs rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9.
Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.
The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.

CHAPTER III COOPERATION BETWEEN COMPETENT AUTHORITIES
Article 8
Cooperation network
The competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems.
The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ("ENISA") shall assist the cooperation network by providing its expertise and advice.
Within the cooperation network the competent authorities shall:
(a) circulate early warnings on risks and incidents in accordance with Article 10;
(b) ensure a coordinated response in accordance with Article 11;
(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;
(d) jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive;
(e) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;
(f) cooperate and exchange information on all relevant matters with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;
(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
(h) organise regular peer reviews on capabilities and preparedness;
(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.
4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2).

Article 9
...
Secure information-sharing system
The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, regarding:
(a) the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and
(b) the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(9), Article 7(2) and Article 7(3).

The Commission shall adopt, by means of implementing acts, decisions on the access of the Member States to this secure infrastructure, pursuant to the criteria referred to in paragraph 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3). Article 10 Early warnings
The competent authorities or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:
(a) they grow rapidly or may grow rapidly in scale;
(b) they exceed or may exceed national response capacity;
(c) they affect or may affect more than one Member State.

In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.

At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol.

The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1. Article 11 Coordinated response
Following an early warning referred to in Article 10 the competent authorities shall, after assessing the relevant information, agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12. The various measures adopted at national level as a result of the coordinated response shall be communicated to the cooperation network.

Article 12 Union NIS cooperation plan
The Commission shall be empowered to adopt, by means of implementing acts, a Union NIS cooperation plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

The Union NIS cooperation plan shall provide for:
(a) for the purposes of Article 10:
– a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the competent authorities;
– a definition of the procedures and the criteria for the assessment of the risks and incidents by the cooperation network;
– the processes to be followed for the coordinated responses under Article 11, including identification of roles and responsibilities and cooperation procedures;
(c) a roadmap for NIS exercises and training to reinforce, validate, and test the plan;

(d) a programme for transfer of knowledge between the Member States in relation to capacity building and peer learning;
(e) a programme for awareness raising and training between the Member States.

The Union NIS cooperation plan shall be adopted no later than one year following the entry into force of this Directive and shall be revised regularly. Article 13 International cooperation
The Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.

Chapter IV
Security of the networks and Information systems of Public Administrations and Market Operators

Article 14 Security requirements and incident notification
Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.

The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.

The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.

The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.12.

Article 15 Implementation and enforcement
Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

Member States shall ensure that the competent authorities have the power to require market operators and public
applications to: (a) provide information needed to assess the security of their networks and information systems, including documented security policies; (b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.

Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

Member States shall ensure that any obligations imposed on public administrations and market operators under this Chapter may be subject to judicial review. Article 16

Standardisation

To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

CHAPTER V FINAL PROVISIONS

Article 17

Sanctions

Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendments affecting them. Member states shall ensure that when a security incident involves personal data, the sanctions are consistent with the sanctions provided by the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Article 18

Exercise of the delegation

The power to adopt the delegated acts is conferred on the Commission subject to the conditions laid down in this Article. The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

The delegation of powers referred to in Articles 9(2), 10(5) and 14(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated act already in force.

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

A delegated act adopted pursuant to Articles 9(2), 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council. Article 19 Committee procedure

The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Article 20 Review

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.

Article 21 Transposition

Member States shall adopt and publish, by [one year and a half after adoption] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. The Member States shall forthwith communicate to the Commission the text of such provisions. They shall apply those measures from [one year and a half after adoption]. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive. Article 22 Entry into force

This Directive shall enter into force on the [twentieth] day following that of its publication in the Official Journal of the European Union.

Article 23 Addressees

This Directive is addressed to the Member States. Done at Brussels, For the European Parliament For the Council The President The President

ANNEX I

Requirements and tasks of the Computer Emergency Response Team (CERT)

The requirements and tasks of the CERT shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:

(1) Requirements for the CERT
(a) The CERT shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.
(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.
(c) The offices of the CERT and the supporting information systems shall be located in secure sites.
(d) A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.
(e) Business continuity:
   - The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.
   - The CERT shall be adequately staffed to ensure availability at all times.
   - The CERT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the CERT to ensure permanent access to the means of communication.
The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

This proposal is presented in connection with the joint Communication of the Commission and High Representative of the Union for Foreign Affairs and Security Policy on a European Cybersecurity Strategy. The objective of the Strategy is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and other EU core values. This proposal is the main action of the Strategy. Further actions under the Strategy in this area focus on raising awareness, developing an internal market for cybersecurity products and services, and fostering R&D investment. These actions will be complemented by others aimed at stepping up the fight against cybercrime and building an international cybersecurity policy for the EU.

1.1. Reasons for and objectives of the proposal

NIS is increasingly important to our economy and society. NIS is also an important precondition to create a reliable environment for worldwide trade in services. However, information systems can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. The Commission’s online public consultation on ‘Improving network and information security in the EU’ found that 57% of respondents had experienced NIS incidents over the previous year that had a serious impact on their activities. Lack of NIS can compromise vital services depending on the integrity of network and information systems. This can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare. Moreover, as a borderless communication instrument, digital information systems, in particular the internet, are interconnected across Member States and play an essential role in facilitating the cross-border movement of goods, services and people. Substantial disruption of these systems in one Member State can affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the completion of the Digital Single Market and the smooth functioning of the Internal Market. The likelihood and frequency of incidents and the inability to ensure efficient protection also undermine public trust and confidence in network and information services for example, the 2012 Eurobarometer on Cybersecurity found that 38% of EU internet users are concerned about the safety of online payments and have changed their behaviour because of concerns with security issues: 18% are less likely to buy goods online and 15% are less likely to use online banking.

The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of
threats and to ensure a common high level of protection in all the Member States. Despite the initiatives undertaken, the Member States have very different levels of capabilities and preparedness, leading to fragmented approaches across the EU. Given the fact that networks and systems are interconnected, the overall NIS of the EU is weakened by those Member States with an insufficient level of protection. This situation also hinders the creation of trust among peers, which is a prerequisite for cooperation and information sharing. As a result, there is cooperation only among a minority of Member States with a high level of capabilities. Therefore, there is currently no effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, leading to insufficient protection against NIS across the EU. Internal Market barriers may also arise, generating compliance costs for companies operating in more than one Member State. Finally, the players managing critical infrastructure or providing services essential to the functioning of our societies are not under appropriate obligations to adopt risk management measures and exchange information with relevant authorities. On the one hand, therefore, businesses lack effective incentives to conduct serious risk management, involving risk assessment and taking appropriate steps to ensure NIS. On the other hand, a large proportion of incidents does not reach the competent authorities and go unnoticed. However, information on incidents is essential for public authorities to react, take appropriate mitigating measures, and set adequate strategic priorities for NIS. The current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. However, many other sectors rely on ICT as an enabler and should therefore be concerned about NIS as well. A number of specific infrastructure and service providers are particularly vulnerable, due to their high dependence on correctly functioning network and information systems. These sectors play an essential role in providing key support services for our economy and society, and the security of their systems is of particular importance to the functioning of the Internal Market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services and public administrations. A step-change is therefore needed in the way NIS is dealt with in the EU. Regulatory obligations are required to create a level playing field and to close existing legislative loopholes. To address these problems and increase the level of NIS within the European Union, the objectives of the proposed Directive are as follows. First, the proposal requires all the Member States to ensure that they have in place a minimum level of national capabilities by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adopting national NIS strategies and national NIS cooperation plans. Secondly, the national competent authorities should cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level. Through this network, Member States should exchange information and cooperate to counter NIS threats and incidents on the basis of the European NIS cooperation plan. Thirdly, based on the model of the Framework Directive for electronic communications, the proposal aims to ensure that a culture of risk management develops and that information is shared between the private and public sectors. Companies in the specific critical sectors outlined above and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. These entities will be required to report to the competent authorities any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods. 1.2. General context Already in 2001, in its Communication Network and Information Security: Proposal for A European Policy Approach, the Commission outlined the increasing importance of NIS. This was followed by the adoption in 2006 of a Strategy for a Secure Information Society, aiming to develop a culture of NIS in Europe. Its main elements were endorsed in a Council Resolution. The Commission further adopted, on 30 March 2009, a Communication on Critical Information Infrastructure protection (CIIP) focusing on the protection of Europe from cyber disruptions by enhancing security. The Communication launched an action plan to support Member States’ efforts to ensure prevention and response. The Action Plan was endorsed in the Presidency Conclusions of the Ministerial Conference on CIIP in Tallinn in 2009. On 18 December 2009 the Council adopted a Resolution on ‘A collaborative European approach to network and information security’. The Digital Agenda for Europe (DAE), adopted in May 2010, and the related Council Conclusions highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of ICT and thus for achieving the objectives of the ‘smart growth’ dimension of the Europe 2020 Strategy. Under its Trust and Security chapter, the DAE emphasised the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructure, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated security mechanisms. In particular, key action 6 of the Digital Agenda for Europe calls for measures aimed at a reinforced and high-level NIS policy. In its Communication on CIIP of March 2011 on ‘Achievements and next steps: towards global cyber-security’, the Commission took stock of the results achieved since the adoption of the CIIP action plan in 2009, concluding that the implementation of the plan showed that purely national approaches to tackling the security and resilience challenges are not sufficient, and that Europe should continue its efforts to build a coherent and cooperative approach across the EU. The 2011 CIIP Communication announced a number of actions, with the Commission calling upon the Member States to set up NIS capabilities and cross-border cooperation. Most of these actions should have been completed by 2012, but have not yet been implemented. In its Conclusions of 27 May 2011 on CIIP, the Council of the European Union stressed the pressing need to make ICT systems and network resilient and secure against all possible disruptions, whether accidental or intentional, to develop across the EU a high level of preparedness, security and resilience capabilities, to upgrade technical competences to allow Europe to meet the challenge of network and information infrastructure protection, and to foster cooperation between the Member States by developing incident cooperation mechanisms between the Member States. 1.3. Existing European Union and international provisions in this area Under Regulation (EC) No 460/2004, the European Community established in 2004 the European Network and Information Security Agency (ENISA), with the aim of contributing to ensuring a high level and developing a culture of NIS within the EUA proposal to modernise the mandate of ENISA was adopted on 30 September 2010 and is under discussion in the Council and the European Parliament. The revised regulatory framework for electronic communications, in force since November 2009, imposes security obligations on electronic communication providers. These obligations had to be transposed at national level by May 2011. All players that are data controllers (for example banks or hospitals) are obliged by the data protection regulatory framework to put in place security measures to protect
personal data. Also, under the 2012 Commission proposal for a General Data Protection Regulation, data controllers would have to report breaches of personal data to the national supervisory authorities. This means that, for example, a NIS security breach affecting the provision of a service without compromising personal data (e.g. an ICT outage at a power company resulting in a blackout) would not have to be notified.

Under Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, the 'European Programme for Critical Infrastructure Protection (EPCIP)' sets out the overall 'umbrella' approach to the protection of critical infrastructures in the EU. The objectives of EPCIP are fully consistent with this proposal and the Directive should apply without prejudice to Directive 2008/114. EPCIP does not oblige operators to report significant breaches of security and does not set up mechanisms for the Member States to cooperate and respond to incidents.

The co-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems, which aims to harmonise the criminalisation of specific types of conduct. It covers only the criminalisation of specific types of conduct and does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact. The present Directive should apply without prejudice to the Directive on attacks against information systems.

On 28 March 2012, the Commission adopted a Communication on the establishment of a European Cybercrime Centre (EC3). This Centre, established on 11 January 2013, is part of the European Police Office (EUROPOL) and acts as the focal point in the fight against cybercrime in the EU. EC3 is intended to pool European cybercrime expertise to support the Member States in capacity building, provide support to Member States’ cybercrime investigations and, in close cooperation with Europol, become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

The European Institutions, agencies and bodies have set up their own Computer Emergency Response Team, called CERT-EU.

At international level, the EU works on cybersecurity at both bilateral and multilateral level. The 2010 EU-US Summit saw the establishment of the EU-US Group on Cybersecurity and Cybercrime. The EU is also active in other relevant multilateral fora, such as the Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITU), the Organisation for Security and Co-operation in Europe (OSCE), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF).

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

2.1. Consultation with interested parties and use of expertise

An online public consultation on ‘Improving NIS in the EU’ ran between 23 July and 15 October 2012. In total, the Commission received 160 responses to the online questionnaire. The key outcome was that stakeholders showed general support for the need to improve NIS across the EU. In particular: 82.8% of respondents expressed the view that governments in the EU should do more to ensure a high level of NIS; 82.8% were of the opinion that users of information and systems were unaware of existing NIS threats and incidents; 66.3% would in principle be in favour of introducing a regulatory requirement to manage NIS risks; and 84.8% said that such requirements should be set at EU level. A high number of respondents thought that it would be important to adopt NIS requirements in the following sectors in particular: banking and finance (91.1%), energy (89.4%), transport (81.7%), health (89.4%), internet services (89.1%), and public administrations (87.5%). Respondents also considered that if a requirement to report NIS security breaches to the national competent authority were introduced, it should be set at EU level (65.1%) and affirmed that public administrations should also be subject to it (93.5%). Finally, respondents affirmed that a requirement to implement NIS risk management in line with the state of the art would entail high costs (63.4%), and that a requirement to report security breaches would cause no significant additional costs (72.3%).

Member States were consulted in a number of relevant Council configurations, in the context of the European Forum for Member States (EFMS), at the Conference on Cybersecurity organised by the Commission and the European External Action Service on 6 July 2012, and in dedicated bilateral meetings convened at the request of individual Member States.

Discussions with the private sector were also held within the European Public-Private Partnership for Resilience and through bilateral meetings. As for the public sector, the Commission held discussions with ENISA and the CERT for the EU institutions.

2.2. Impact assessment

The Commission has carried out an impact assessment of three policy options:

Option 1: Business as usual (baseline scenario): maintaining the current approach;
Option 2: Regulatory approach, consisting of a legislative proposal establishing a common EU legal framework for NIS regarding Member State capabilities, mechanisms for EU-level cooperation, and requirements for key private players and public administrations;
Option 3: Mixed approach, combining voluntary initiatives for Member State NIS capabilities and mechanisms for EU-level cooperation with regulatory requirements for key private players and public administrations.

The Commission concluded that Option 2 would have the strongest positive impacts, as it would considerably improve the protection of EU consumers, business and governments against NIS incidents. In particular, the obligations placed on the Member States would ensure adequate preparedness at national level and would contribute to a climate of mutual trust, which is a precondition for effective cooperation at EU level. The setting up of mechanisms for cooperation at EU level via the network would deliver coherent and coordinated prevention and response to cross-border NIS incidents and risks. The introduction of requirements to implement NIS risk management for public administrations and key private players would create a strong incentive to manage security risks effectively. The obligation to report NIS incidents with a significant impact would enhance the ability to respond to incidents and foster transparency. Moreover, by putting its own house in order, the EU would be able to extend its international reach and become an even more credible partner for cooperation at bilateral and multilateral level. The EU would hence also be better placed to promote fundamental rights and EU core values abroad.

The quantitative assessment showed that Option 2 would not impose a disproportionate burden on Member States. The costs for the private sector would also be limited since many of the entities concerned are already supposed to comply with existing security requirements (namely the obligation for data controllers to take technical and organisational measures to secure personal data, including NIS measures). Existing spending on security in the private sector has also been taken into account.

This proposal observes the principles recognised by the Charter of Fundamental Rights of the European Union notably, the right to respect for private life and communications, the protection for personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal basis
The European Union is empowered to adopt measures with the aim of establishing or ensuring the functioning of the Internal Market, in accordance with the relevant provisions of the Treaties (Article 26 of the Treaty on the Functioning of the European Union — TFEU). Under Article 114 TFEU, the EU can adopt 'measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market'.

As indicated above, network and information systems play an essential role in facilitating the cross-border movement of goods, services and people. They are often interconnected, and the internet is global in nature. Given this intrinsic transnational dimension, a disruption in one Member State can also affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the Internal Market.

The EU legislator has already recognised the need to harmonise NIS rules to ensure the development of the Internal Market. In particular, this was the case for Regulation 460/2004 establishing ENISA, which is based on Article 114 TFEU.

The disparities resulting from uneven NIS national capabilities, policies and level of protection across the Member States lead to barriers to the Internal Market and justify EU action.

3.2. Subsidiarity

European intervention in the area of NIS is justified by the subsidiarity principle. Firstly, considering the cross-border nature of NIS, non-intervention at EU level would lead to a situation where each Member State would act alone, disregarding the interdependencies among EU network and information systems. An appropriate degree of coordination among the Member States would ensure that NIS risks could be well managed in the cross-border context in which they arise.

Divergences in NIS regulations represent a barrier to companies wanting to operate in several countries and to the achievement of global economies of scale. Secondly, regulatory obligations at EU level are needed to create a level playing field and close legislative loopholes. A purely voluntary approach has resulted in cooperation only among a minority of Member States with a high level of capabilities. In order to involve all the Member States, it is necessary to ensure that they all have the required minimum level of capability. NIS measures adopted by governments need to be consistent with one other and be coordinated to contain and minimise the consequences of NIS incidents.

Within the network, through exchange of best practices and continuous involvement of ENISA, the competent authorities and the Commission will cooperate to facilitate a convergent implementation of the Directive across the EU. In addition, concerted NIS policy actions can have a strong positive impact for the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy. Action at EU level would therefore improve the effectiveness of existing national policies and facilitate their development.

The proposed measures are also justified on grounds of proportionality. The requirements for the Member States are set at the minimum level necessary to achieve adequate preparedness and to enable cooperation based on trust. This also enables Member States to take due account of national specificities and ensures that the common EU principles are applied in a proportionate manner. The wide scope of application will allow the Member States to implement the Directive in light of the actual risks faced at national level as identified in the national NIS strategy. The requirements to implement risk management target only critical entities and impose measures that are proportionate to the risks. The public consultation underlined the importance of ensuring the security of these critical entities. The reporting requirements would concern only incidents with a significant impact. As indicated above, the measures would not impose disproportionate costs, as many of these entities as data controllers are already required by the current data protection rules to secure the protection of personal data.

To avoid imposing a disproportionate burden on small operators, in particular on SMEs, the requirements are proportionate to the risks presented by the network or information system concerned and should not apply to micro enterprises. The risks will have to be identified in the first place by the entities subject to these obligations, which will have to decide on the measures to be adopted to mitigate such risks.

The stated objectives can be better achieved at EU level, rather than by the Member States alone, in view of the cross-border aspects of NIS incidents and risks. Therefore, the EU may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, the proposed Directive does not go beyond what is necessary in order to achieve those objectives.

To achieve the objectives, the Commission should be empowered to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the European Union, in order to supplement or amend certain non-essential elements of the basic act. The Commission’s proposal also strives to support a process of proportionality in the implementation of the obligations placed upon private and public operators.

In order to ensure uniform conditions for the implementation of the basic act, the Commission should be empowered to adopt implementing acts in accordance with Article 291 of the Treaty on the Functioning of the European Union, in order to supplement or amend certain non-essential elements of the Directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

4. BUDGETARY IMPLICATIONS

Cooperation and exchange of information between Member States would be supported by a secure infrastructure. The proposal will have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement this under the MFF 2014-2020. The one-off cost is estimated to be EUR 1 250 000 and would be borne by the EU budget, budget line 09.03.02 (to promote the interconnection and interoperability of national public services online as well as access to such networks — Chapter 09.03, Connecting Europe Facility — telecommunication networks) on condition that sufficient funds are available under CEF. Alternatively, Member States can either share the one-off cost of adapting an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately EUR 10 million per year.
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

1. INTRODUCTION

1.1. Context

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard the private sector against the private sector and individuals. Cybercriminals are motivated by profit and are highly skilled in their techniques. They can cause significant damage and disrupt the economy. Cybersecurity can only be sound and effective if the same laws and norms that apply in other areas of our daily life are applied to cyberspace. The same laws and norms that apply in other areas of our daily life are applied to cyberspace. The same laws and norms that apply in other areas of our daily life are applied to cyberspace.

Information and communications technology has become the backbone of our economic growth and a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

By completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year; an average of €1000 per person. For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cybersecurity strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU’s vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens’ rights to make the EU’s online environment the safest in the world.

1.2. Principles for cybersecurity

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally.

The EU’s core values apply as much in the digital as in the physical world.

The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain. Protecting fundamental rights, freedom of expression, personal data and privacy.

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals’ rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals’ rights in this field.

Access for all

Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet’s integrity and security must be guaranteed to allow safe access for all.

Democratic and efficient multi-stakeholder governance

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach. A shared responsibility to ensure security.
The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

2. STRATEGIC PRIORITIES AND ACTIONS

The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU’s overall performance. These actions are both short and long term, they include a variety of policy tools and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

2.1. Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activity carried out to date further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS). The European Network and Information Security Agency ENISA was established in 2004 and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament. In addition, the Framework Directive for electronic communications requires providers of electronic communications to appropriately manage the risks to their networks and the security of their information. Meanwhile, the EU data protection legislation requires data controllers to ensure data protection requirements and safeguards, including measures related to security, and in the field of publicly available e-communication services, data controllers have to notify incidents involving a breach of personal data to the competent national authorities.

Despite progress based on voluntary commitments, there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness. This strategy is accompanied by a proposal for legislation to notably:

- Establish common minimum requirements for NIS at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning CERT; and adopt a national NIS strategy and a national NIS cooperation plan. Capacity building and coordination also concern the EU institutions: a Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies (“CERT-EU”) was permanently established in 2012.
- Set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities. National NIS competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a Union NIS cooperation plan, designed to respond to cyber incidents with cross-border dimension. This cooperation will also build upon the progress made in the context of the ‘European Forum for Member States (EFMS),’ which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.
- Improve preparedness and engagement of the private sector.

Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cybersecurity capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector. However, private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions. The proposed legislation therefore aims at making sure that players in a number of key areas (namely energy, transport, banking, stock exchanges, and enablers of key Internet services, as well as public administrations) assess the cybersecurity risks they face, ensure networks and information systems are reliable and resilient via appropriate risk management, and share the identified information with the national NIS competent authorities. The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point. Those entities would have to report, to the national NIS competent authorities, incidents with a significant impact on the continuity of core services and supply of goods relying on network and information systems. National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. NIS competent authorities should in turn report incidents of a suspected serious criminal nature to law enforcement authorities. The national competent authorities should also regularly publish on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses. Legal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices.

In particular, the European Public-Private Partnership for Resilience (EPPR) is a sound and valid platform at EU level and should be further expanded.

The Connecting Europe Facility (CEF) would provide financial support for key infrastructure, linking up Member States’ NIS capabilities and so making it easier to cooperate across the EU.

Finally, cyber incident exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The first exercise involving the Member States was carried out in 2010 (“Cyber Europe 2010”) and a second exercise, involving also the private sector, took place in October 2012 (“Cyber Europe 2012”). An EU-US table top exercise was carried out in November 2014 (“Cyber Atlantic 2011”). Further exercises are planned for the coming years, including with international partners.

The Commission will:
- Continue its activities, carried out by the Joint Research Centre, with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.
- Launch an EU-funded pilot project early in 2013 on fighting botnets and malware, to provide a framework for coordination
and cooperation between EU Member States, private sector organisations such as Internet Service Providers, and international partners.

The Commission asks ENISA to:
- Assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Examine in 2013 the feasibility of Computer Security Incident Response Team (CSIRTs) for the EU
- Continue supporting the Member States and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises.

The Commission invites the European Parliament and the Council to:
- Swiftly adopt the proposal for a Directive on a common high level of Network and Information Security (NIS) across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS.

The Commission asks industry to:
- Take leadership in investing in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in particular through public-private partnerships like EPST and Trust in Digital Life (TDL).

Raising awareness

Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.

Several initiatives have been developed in recent years and should be continued. In particular, ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness. In October 2012, ENISA, with some Member States, piloted the "European Cybersecurity Month". Raising awareness is one of the areas the EU-US working group on cybersecurity and cybercrime is taking forward, and is also essential in the context of the Safer Internet Programme (focused on the safety of children online).

The Commission asks ENISA to:
- Propose in 2013 a roadmap for a "Network and Information Security Driving Licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators).

The Commission will:
- Organise, with the support of ENISA, a cybersecurity championship in 2014, where university students will compete in proposing NIS solutions.

The Commission invites the Member States to:
- Organise a yearly cybersecurity month with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cybersecurity month will be organised starting in 2014.
- Step up national efforts on NIS education and training, by introducing training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations. The Commission invites industry to:
- Promote cybersecurity awareness at all levels, both in business practices and in the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.

2.2. Drastically reducing cybercrime

The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat.

Strong and effective legislation

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation. The EU has already adopted legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography. The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

The Commission will:
- Ensure swift transposition and implementation of the cybercrime-related directives.
- Urge those Member States that have not yet ratified the Council of Europe’s Budapest Convention on Cybercrime to ratify and implement its provisions as early as possible.

Enhanced operational capability to combat cybercrime

The evolution of cybercrime techniques has accelerated rapidly: law enforcement agencies cannot combat cybercrime with outdated operational tools. Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units.

The Commission will:
- Through its funding programmes, support the Member States to identify gaps and strengthen their capability to investigate and combat cybercrime. The Commission will furthermore support bodies that make the link between research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States.

Together with the Member States, coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime (e.g. with respect to the development and use of forensic tools or to threat analysis)

Work closely with the recently launched European Cybercrime Centre (EC3), within Europol and with Eurojust to align such policy approaches with best practices on the operational side.

Improved coordination at EU level

The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond.

The Commission will:
- Support the recently launched European Cybercrime Centre (EC3) as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community.

Support efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned
Names and Numbers (ICANN) in compliance with Union law, including the rules on data protection.

Build on recent legislation to continue strengthening the EU’s efforts to tackle child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children and has, together with EU and non-EU countries, launched a Global Alliance against Child Sexual Abuse Online. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3. The Commission asks Europol (EC3) to:

- Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field.

The Commission asks Europol (EC3) to:
- Coordinate the design and planning of training courses to equip law enforcement with the knowledge and expertise to effectively tackle cybercrime.

The Commission asks Europol to:
- Coordinate closely, inter alia through the exchange of information, in order to increase their effectiveness in combating cybercrime, in accordance with their respective mandates and competence.

2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States’ defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats.

Given the nature of cybersecurity, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:

Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability.

Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues; Promote dialogue and coordination between civilian and military actors in the EU - with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority.

Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

2.4. Develop industrial and technological resources for cybersecurity

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

Promoting a Single Market for cybersecurity products

A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. It seems however that many players still regard security as little more than an additional burden and there is limited demand for security solutions. There need to be appropriate cybersecurity performance requirements implemented across the whole value chain for ICT products used in Europe. The negative impact of supply chain attacks could be mitigated if the market for ICT products and services was subject to common standards for cybersecurity that would enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge. Also, the obligations set out in the proposed NIS Directive would significantly contribute to step up business competitiveness in the sectors covered.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses.

Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking into due account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure). Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI) of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players.

The Commission will:
Launch in 2013 a public-private platform on NIS solutions to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products in Europe.
Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform.
Examine how major providers of ICT hardware and software could inform national competent authorities on detected
vulnerabilities that could have significant security implications. The Commission asks ENISA to:

1. Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

The Commission invites public and private stakeholders to:

- Stimulate the development and adoption of industry-led security standards, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new generations of software and hardware should be equipped with stronger, embedded and user-friendly security features.

- Develop industry-led standards for companies’ performance on cybersecurity and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market.

- Fostering R&D investments and innovation R&D can support a strong industrial policy, promote a trustworthy European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges, take into account the constant evolution of user needs and reap the benefits of the use of these technologies. It should also continue to provide incentives for the development of cryptography. This has to be complemented by efforts to translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

The EU should make the best of the Horizon 2020 Framework Programme for Research and Innovation, to be launched in 2014. The Commission’s proposal contains specific objectives for trustworthy ICT as well as for combating cyber-crime, which are in line with this strategy. Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation).

The Commission will:

- Use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.

- Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and incentivise the Member States to invest more in R&D. The Commission invites the Member States to:

  - Develop, by the end of 2013, good practices to use the purchasing power of public administrations (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services.

- Promote early involvement of industry and academia in developing and coordinating solutions. This should be done by making the most of Europe’s Industrial Base and associated R&D technological innovations, and be coordinated between the research agendas of civilian and military organisations.

The Commission asks Europol and ENISA to:

1. Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.

The Commission invites public and private stakeholders to:

- Develop, in cooperation with the insurance sector, harmonised metrics for calculating risk premiums, that would enable companies that have made investments in security to benefit from lower risk premiums.

2.5. Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop responsible cyberspace behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The EU international engagement in cyber issues will be guided by the EU’s core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector. EU consultations with international partners on cyber issues should be designed, coordinated and implemented to address the threats to existing and future cyber systems. The EU should seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility, and launch international initiatives to improve global coordination in this field. The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour.

The EU does not call for the creation of new international legal instruments for cyber issues.

The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace. To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field. If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human rights law will apply to the case at hand. Developing capacity building on cybersecurity and resilient information infrastructures in third countries
The smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises, and so on. The EU will contribute towards this goal by intensifying the ongoing international efforts to strengthen Critical Information Infrastructure Protection (CIPP) cooperation networks involving governments and the private sector. Not all parts of the world benefit from the positive effects of the Internet due to a lack of open, secure, interoperable and reliable access. The European Union will therefore continue to support countries' efforts in their quest to develop the access and use of the Internet for their people, to ensure its integrity and security and to effectively fight cybercrime.

In cooperation with the Member States, the Commission and the High Representative will:

1. Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues; Support the development of norms of behaviour and confidence building measures in cybersecurity. Facilitate dialogues on how to apply existing international law in cyberspace and promote the Budapest Convention to address cybercrime; Support the promotion and protection of fundamental rights, including access to information and expression online, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance; d) empowering stakeholders to use communication technology to promote fundamental rights; Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts; Utilise different EU aid instruments for cybersecurity capacity building, by complementing, assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries; Increase policy coordination and information sharing through the international Critical Information Infrastructure Protection (CIPP) networks such as the Meridian network, the EDA cyber defence project team can be used as the vector of communication technology among the Member States, ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

2. Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

3. ROLES\&RESPONSIBILITIES

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU level and work together to strengthen cybersecurity. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive fashion, activities should span across three key pillars— NIS, law enforcement, and defence—which also operate within different legal frameworks:

**Industry Academia**

3.1. Coordination between NIS competent authorities / CERTs, law enforcement and defence

**National level**

Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cybersecurity, and given the importance of involving the private sector, coordination at national level should be optimised across ministries. Member States should set out in their national cybersecurity strategies the roles and responsibilities of their various national entities. Information sharing between national entities and with the private sector should be encouraged, to enable the Member States and the private sector to maintain an overall view of different threats and get a better understanding of new trends and techniques used both to commit cyber-attacks and react to them more swiftly. By establishing national NIS cooperation plans to be activated in the case of cyber incidents, the Member States should be able to clearly allocate roles and responsibilities and optimise response actions.

**EU level**

Just as at national level, there are at EU level a number of actors dealing with cybersecurity. In particular, the ENISA, Europol/EC3 and EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be enhanced among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

Informal channels for coordination and collaboration will be complemented by more structural links. EU military staff and the EDA cyber defence project team can be used as the vector for coordination in defence. The Programme Board of Europol/EC3 will bring together among others the EUROJUST, CEPOL, the Member States, ENISA and the Commission, and offer the chance to share their distinct know-how and to make sure EC3's actions are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders. The new mandate of ENISA should make it possible to increase its links with Europol/EC3 and EDA for coordination with EU and international partners and with European stakeholders. Most importantly, the Commission's legislative proposal on NIS would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities.

**International**

The Commission and the High Representative ensure, together with the Member States, coordinated international action in the field of cybersecurity. In so doing, the Commission and the High Representative will uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

3.2. EU support in case of a major cyber incident or attack

Major cyber incidents are likely to have an impact on EU governments, business and individuals. As a result of this strategy, and in particular the proposed directive on NIS, the prevention, detection and response to cyber incidents should improve and Member States and the Commission should keep each other more closely informed about major cyber incidents or attacks. However, the response mechanisms
will differ depending on the nature, magnitude and cross-border implications of the incident.
If the incident has a serious impact on the business continuity, the NIS directive proposes that national or Union NIS cooperation plans be triggered, depending on the cross-border nature of the incident. The network of NIS competent authorities would be used in that context to share information and support. This would enable preservation and/or restoration of affected networks and services.
If the incident seems to relate to a crime, Europol/EC3 should be informed so that they, together with the law enforcement authorities from the affected countries, can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted.
If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).
If the incident seems having compromised personal data, the national Data Protection Authorities or the national regulatory authority pursuant to Directive 2002/58/EC should be involved.

Finally, the handling of cyber incidents and attacks will benefit from contact networks and support from international partners. This may include technical mitigation, criminal investigation, or activation of crisis management response mechanisms.

4. CONCLUSION AND FOLLOW-UP
This proposed cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world. This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

The Commission and the High Representative therefore invite the Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. Strong support and commitment is also needed from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights. The time to act is now. The Commission and the High Representative are determined to work together with all actors to deliver the security needed for Europe. To ensure that the strategy is being implemented promptly and assessed in the face of possible developments, they will gather together all relevant parties in a high-level conference and assess progress in 12 months.
VII. Copyright Law

Berne Convention for the Protection of Literary and Artistic Works


The countries of the Union, being equally animated by the desire to protect, in as effective and uniform a manner as possible, the rights of authors in their literary and artistic works, recognizing the importance of the work of the Revision Conference held at Stockholm in 1967, have resolved to revise the Act adopted by the Stockholm Conference, while maintaining without change Articles 1 to 20 and 22 to 26 of that Act. Consequently, the undersigned Plenipotentiaries, having presented their full powers, recognized as in good and due form, have agreed as follows:

Article 1
[Establishment of a Union]

1. Each Article and the Appendix have been given titles to facilitate their identification. There are no titles in the signed (English) text. The countries to which this Convention applies constitute a Union for the protection of the rights of authors in their literary and artistic works.

Article 2
[Protected Works]

1. "Literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatico-musical works; choreographic works and entertainments in dumb show; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science.

2. It shall, however, be a matter for legislation in the countries of the Union to prescribe that works in general or any specified categories of works shall not be protected unless they have been fixed in some material form.

3. Translations, adaptations, arrangements of music and other alterations of a literary or artistic work shall be protected as original works without prejudice to the copyright in the original work.

4. It shall be a matter for legislation in the countries of the Union to determine the protection to be granted to official texts of a legislative, administrative and legal nature, and to official translations of such texts.

5. Collections of literary or artistic works such as encyclopaedias and anthologies which, by reason of the selection and arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections.

6. The works mentioned in this Article shall enjoy protection in all countries of the Union. This protection shall operate for the benefit of the author and his successors in title.

7. Subject to the provisions of Article 7(4) of this Convention, it shall be a matter for legislation in the countries of the Union to determine the extent of the application of their laws to works of applied art and industrial designs and models, as well as the conditions under which such works, designs and models shall be protected. Works protected in the country of origin solely as designs and models shall be entitled in another country of the Union only to such special protection as is granted in that country to designs and models; however, if no such special protection is granted in that country, such works shall be protected as artistic works.

8. The protection of this Convention shall not apply to news of the day or to miscellaneous facts having the character of mere items of press information.

Article 2bis
[Possible Limitation of Protection of Certain Works]

1. Certain speeches; 2. Certain uses of lectures and addresses; 3. Right to make collections of such works

2. It shall also be a matter for legislation in the countries of the Union to determine the conditions under which lectures, addresses and other works of the same nature which are delivered in public may be reproduced by the press, broadcast, communicated to the public by wire and made the subject of public communication as envisaged in Article 11bis(1) of this Convention, when such use is justified by the informative purpose.

3. Nevertheless, the author shall enjoy the exclusive right of making a collection of his works mentioned in the preceding paragraphs.

Article 3
The protection of this Convention shall apply to:
(a) authors who are nationals of one of the countries of the Union, for their works, whether published or not;
(b) authors who are not nationals of one of the countries of the Union, for their works first published in one of those countries, or simultaneously in a country outside the Union and in a country of the Union.
(2) Authors who are not nationals of one of the countries of the Union but who have their habitual residence in one of them shall, for the purposes of this Convention, be assimilated to nationals of that country.
(3) The expression "published works" means works published with the consent of their authors, whatever may be the means of manufacture of the copies, provided that the availability of such copies has been such as to satisfy the reasonable requirements of the public, having regard to the nature of the work. The performance of a dramatic, dramatico-musical, cinematographic or musical work, the public recitation of a literary work, the communication by wire or the broadcasting of literary or artistic works, the exhibition of a work of art and the construction of a work of architecture shall not constitute publication.
(4) A work shall be considered as having been published simultaneously in several countries if it has been published in two or more countries within thirty days of its first publication.

Article 4
[Criteria of Eligibility for Protection of Cinematographic Works, Works of Architecture and Certain Artistic Works]

The protection of this Convention shall apply, even if the conditions of Article 3 are not fulfilled, to:
(a) authors of cinematographic works the maker of which has his headquarters or habitual residence in one of the countries of the Union;
(b) authors of works of architecture erected in a country of the Union or other artistic works incorporated in a building or other structure located in a country of the Union.

Article 5
[Rights Guaranteed: 1. and 2. Outside the country of origin; 3. In the country of origin; 4. "Country of origin"]

(1) Authors shall enjoy, in respect of works for which they are protected under this Convention, in countries of the Union other than the country of origin, the rights which their respective laws do now or may hereafter grant to their nationals, as well as the rights specially granted by this Convention.
(2) The enjoyment and the exercise of these rights shall not be subject to any formalities; such enjoyment and such exercise shall be independent of the existence of protection in the country of origin of the work. Consequently, apart from the provisions of this Convention, the extent of protection, as well as the means of redress afforded to the author to protect his rights, shall be governed exclusively by the laws of the country where protection is claimed.
(3) Protection in the country of origin is governed by domestic law. However, when the author is not a national of the country of origin of the work for which he is protected under this Convention, he shall enjoy in that country the same rights as national authors.
(4) The country of origin shall be considered to:
(a) in the case of works first published in a country of the Union, that country; in the case of works published simultaneously in several countries of the Union which grant different terms of protection, the country whose legislation grants the shortest term of protection;
(b) in the case of works published simultaneously in a country outside the Union and in a country of the Union, the latter country;
(c) in the case of unpublished works or of works first published in a country outside the Union, without simultaneous publication in a country of the Union, the country of the Union of which the author is a national, provided that:
(i) when these are cinematographic works the maker of which has his headquarters or his habitual residence in a country of the Union, the country of origin shall be that country, and
(ii) when these are works of architecture erected in a country of the Union or other artistic works incorporated in a building or other structure located in a country of the Union, the country of origin shall be that country.

Article 6
[Possible Restriction of Protection in Respect of Certain Works of Nationality of Certain Countries Outside the Union: 1. In the country of the first publication and in other countries; 2. No retroactivity; 3. Notice]

(1) Where any country outside the Union fails to protect in an adequate manner the works of authors who are nationals of one of the countries of the Union, the latter country may restrict the protection given to the works of authors who are, at the date of the notification thereof, nationals of the other country and are not habitually resident in one of the countries of the Union. If the country of first publication avails itself of this right, the other countries of the Union shall not be required to grant to works thus subjected to special treatment a wider protection than that granted to them in the country of first publication.
(2) No restrictions introduced by virtue of the preceding paragraph shall affect the rights which an author may have acquired in respect of a work published in a country of the Union before such restrictions were put into force.
(3) The countries of the Union which restrict the grant of copyright in accordance with this Article shall give notice thereof to the Director General of the World Intellectual Property Organization (hereinafter designated as "the Director General") by a written declaration specifying the countries in regard to which protection is restricted, and the restrictions to which rights of authors who are nationals of those countries are subjected. The Director General shall immediately communicate this declaration to all the countries of the Union.

Article 6bis
[Moral Rights: 1. To claim authorship; to object to certain modifications and other derogatory actions; 2. After the author's death; 3. Means of redress]

(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.
(2) The rights granted to the author in accordance with the preceding paragraph shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the country where protection is claimed. However, those countries whose legislation, at the moment of their ratification of or accession to this Act, does not provide for the protection after the death of the author of all the rights set out in the preceding paragraph may provide that some of these rights may, after his death, cease to be maintained.
(3) The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed.
Article 7
[Term of Protection: 1. Generally; 2. For cinematographic works; 3. For anonymous and pseudonymous works; 4. For photographic works and works of applied art; 5. Starting date of computation; 6. Longer terms; 7. Shorter terms; 8. Applicable law; 'comparison' of terms]

(1) The term of protection granted by this Convention shall be the life of the author and fifty years after his death.

(2) However, in the case of cinematographic works, the countries of the Union may provide that the term of protection shall expire fifty years after the work has been made available to the public with the consent of the author, or, failing such an event within fifty years from the making of such a work, fifty years after the making.

(3) In the case of anonymous or pseudonymous works, the term of protection granted by this Convention shall expire fifty years after the work has been lawfully made available to the public. However, when the pseudonym adopted by the author leaves no doubt as to his identity, the term of protection shall be that provided in paragraph (1). If the author of an anonymous or pseudonymous work discloses his identity during the above-mentioned period, the term of protection applicable shall be that provided in paragraph (1). The countries of the Union shall not be required to protect anonymous or pseudonymous works in respect of which it is reasonable to presume that their author has been dead for fifty years.

(4) It shall be a matter for legislation in the countries of the Union to determine the term of protection of photographic works and that of works of applied art in so far as they are protected as artistic works; however, this term shall last at least until the end of a period of twenty-five years from the making of such a work.

(5) The term of protection subsequent to the death of the author and the terms provided by paragraph (2), paragraph (3) and paragraph (4) shall run from the date of death or of the event referred to in those paragraphs, but such terms shall always be deemed to begin on the first of January of the year following the date of such event.

(6) The countries of the Union may grant a term of protection in excess of those provided by the preceding paragraphs.

(7) Those countries of the Union bound by the Rome Act of this Convention which grant, in their national legislation in force at the time of signature of the present Act, shorter terms of protection than those provided for in the preceding paragraphs shall have the right to maintain such terms when ratifying or acceding to the present Act.

(8) In any case, the term shall be governed by the legislation of the country where protection is claimed; however, unless the legislation of that country otherwise provides, the term shall not exceed the term fixed in the country of origin of the work.

Article 7bis
[Term of Protection for Works of Joint Authorship]

The provisions of the preceding Article shall also apply in the case of a work of joint authorship, provided that the terms measured from the death of the author shall be calculated from the death of the last surviving author.

Article 8
[Right of Translation]

Authors of literary and artistic works protected by this Convention shall enjoy the exclusive right of making and of authorizing the translation of their works throughout the term of protection of their rights in the original works.

Article 9

(1) Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form.

(2) It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

(3) Any sound or visual recording shall be considered as a reproduction for the purposes of this Convention.

Article 10
[Certain Free Uses of Works: 1. Quotations; 2. Illustrations for teaching; 3. Indication of source and author]

(1) It shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries.

(2) It shall be a matter for legislation in the countries of the Union, and for special agreements existing or to be concluded between them, to permit the utilization, to the extent justified by the purpose, of literary or artistic works by way of illustration in publications, broadcasts or sound or visual recordings for teaching, provided such utilization is compatible with fair practice.

(3) Where use is made of works in accordance with the preceding paragraphs of this Article, mention shall be made of the source, and of the name of the author if it appears thereon.

Article 10bis
[Further Possible Free Uses of Works: 1. Of certain articles and broadcast works; 2. Of works seen or heard in connection with current events]

(1) It shall be a matter for legislation in the countries of the Union to permit the reproduction by the press, the broadcasting or the communication to the public by wire of articles published in newspapers or periodicals on current economic, political or religious topics, and of broadcast works of the same character, in cases in which the reproduction, broadcasting or such communication thereof is not expressly reserved. Nevertheless, the source must always be clearly indicated; the legal consequences of a breach of this obligation shall be determined by the legislation of the country where protection is claimed.

(2) It shall also be a matter for legislation in the countries of the Union to determine the conditions under which, for the purpose of reporting current events by means of photography, cinematography, broadcasting or communication to the public by wire, literary or artistic works seen or heard in the course of the event may, to the extent justified by the informative purpose, be reproduced and made available to the public.

Article 11
[Certain Rights in Dramatic and Musical Works: 1. Right of public performance and of communication to the public of a performance; 2. In respect of translations]

(1) Authors of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorizing:

(i) the public performance of their works, including such public performance by any means or process;

(ii) any communication to the public of the performance of their works.

(2) Authors of dramatic or dramatico-musical works shall enjoy, during the full term of their rights in the original works, the same rights with respect to translations thereof.

Article 11bis
[Broadcasting and Related Rights: 1. Broadcasting and other wireless communications, public communication of broadcast works; 2. Re-transmission and recording of works protected by this Convention]

(1) Broadcasting and related rights shall be recognized for the purpose of the exploitation of works protected by this Convention.
by wire or rebroadcast, public communication of broadcast by loudspeaker or analogous instruments; 2. Compulsory licenses; 3. Recording; ephemeral recordings]

(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing:
(i) the broadcasting of their works or the communication thereof to the public by any other means of wireless diffusion of signs, sounds or images;
(ii) any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one;
(iii) the public communication by loudspeaker or any other analogous instrument transmitting, by signs, sounds or images, the broadcast of the work.
(2) It shall be a matter for legislation in the countries of the Union to determine the conditions under which the rights mentioned in the paragraph 1 may be exercised, but these conditions shall apply only in the countries where they have been prescribed. They shall not in any circumstances be prejudicial to the moral rights of the author, nor to his right to obtain equitable remuneration which, in the absence of agreement, shall be fixed by competent authority.
(3) In the absence of any contrary stipulation, permission granted in accordance with paragraph (1) of this Article shall not imply permission to record, by means of instruments recording sounds or images, the work broadcast. It shall, however, be a matter for legislation in the countries of the Union to determine the regulations for ephemeral recordings made by a broadcasting organization by means of its own facilities and used for its own broadcasts. The preservation of these recordings in official archives may, on the ground of their exceptional documentary character, be authorized by such legislation.

Article 11ter
[Certain Rights in Literary Works: 1. Right of public recitation and of communication to the public of a recitation; 2. In respect of translations]
(1) Authors of literary works shall enjoy the exclusive right of authorizing:
(i) the public recitation of their works, including such public recitation by any means or process;
(ii) any communication to the public of the recitation of their works.
(2) Authors of literary works shall enjoy, during the full term of their rights in the original works, the same rights with respect to translations thereof.

Article 12
[Right of Adaptation, Arrangement and Other Alteration]
Authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works.

Article 13
[Possible Limitation of the Right of Recording of Musical Works and Any Words Pertaining Thereto: 1. Compulsory licenses; 2. Transitory measures; 3. Seizure on importation of copies made without the author's permission]
(1) Each country of the Union may impose for itself reservations and conditions on the exclusive right granted to the author of a musical work and to the author of any words, the recording of which together with the musical work has already been authorized by the latter, to authorize the sound recording of that musical work, together with such words, if any; but all such reservations and conditions shall apply only in the countries which have imposed them and shall not, in any circumstances, be prejudicial to the rights of these authors to obtain equitable remuneration which, in the absence of agreement, shall be fixed by competent authority.
(2) Recordings of musical works made in a country of the Union in accordance with Article 13(3) of the Conventions signed at Rome on June 2, 1928, and at Brussels on June 26, 1948, may be reproduced in that country without the permission of the author of the musical work until a date two years after that country becomes bound by this Act.
(3) Recordings made in accordance with paragraph (1) and paragraph (2) of this Article and imported without permission from the parties concerned into a country where they are treated as infringing recordings shall be liable to seizure.

Article 14
[Cinematographic and Related Rights: 1. Cinematographic adaptation and reproduction; distribution; public performance and public communication by wire of works thus adapted or reproduced; 2. Adaptation of cinematographic productions; 3. No compulsory licenses]
(1) Authors of literary or artistic works shall have the exclusive right of authorizing:
(i) the cinematographic adaptation and reproduction of these works, and the distribution of the works thus adapted or reproduced;
(ii) the public performance and communication to the public by wire of the works thus adapted or reproduced.
(2) The adaptation into any other artistic form of a cinematographic production derived from literary or artistic works shall, without prejudice to the authorization of the author of the cinematographic production, remain subject to the authorization of the authors of the original works.
(3) The provisions of Article 13(1) shall not apply.

Article 14bis
[Special Provisions Concerning Cinematographic Works: 1. Assimilation to "original" works; 2. Ownership; limitation of certain rights of certain contributors; 3. Certain other contributors]
(1) Without prejudice to the copyright in any work which may have been adapted or reproduced, a cinematographic work shall be protected as an original work. The owner of copyright in a cinematographic work shall enjoy the same rights as the author of an original work, including the rights referred to in the preceding Article.
(2) (a) Ownership of copyright in a cinematographic work shall be a matter for legislation in the country where protection is claimed.
(b) However, in the countries of the Union which, by legislation, include among the owners of copyright in a cinematographic work authors who have brought contributions to the making of the work, such authors, if they have undertaken to bring such contributions, may not, in the absence of any contrary or special stipulation, object to the reproduction, distribution, public performance, communication to the public by wire, broadcasting or any other communication to the public, or to the subtitling or dubbing of texts, of the work.
(c) The question whether or not the form of the undertaking referred to above should, for the application of the preceding subparagraph (b), be in a written agreement or a written act of the same effect shall be a matter for the legislation of the country where the maker of the cinematographic work has his headquarters or habitual residence. However, it shall be a matter for the legislation of the country of the Union where protection is claimed to provide that the said undertaking shall be in a written agreement or a written act of the same effect. The countries whose legislation so provides shall notify the Director General by means of a written declaration, which will be immediately communicated by him to all the other countries of the Union.
(d) By "contrary or special stipulation" is meant any restrictive condition which is relevant to the aforesaid undertaking.

(3) Unless the national legislation provides to the contrary, the provisions of paragraph (2)(b) above shall not be applicable to authors of scenarios, dialogues and musical works created for the making of the cinematographic work, or to the principal director thereof. However, those countries of the Union whose legislation does not contain rules providing for the application of the said paragraph (2)(b) to such director shall notify the Director General by means of a written declaration, which will be immediately communicated by him to all the other countries of the Union.

Article 14ter

(1) The author, or after his death the persons or institutions authorized by national legislation, shall, with respect to original works of art and original manuscripts of writers and composers, enjoy the inalienable right to an interest in any sale of the work subsequent to the first transfer by the author of the work.

(2) The protection provided by the preceding paragraph may be claimed in a country of the Union only if legislation in the country to which the author belongs so permits, and to the extent permitted by the country where this protection is claimed.

(3) The procedure for collection and the amounts shall be matters for determination by national legislation.

Article 15
[Right to Enforce Protected Rights: 1. Where author's name is indicated or where pseudonym leaves no doubt as to author's identity; 2. In the case of cinematographic works; 3. In the case of anonymous and pseudonymous works; 4. In the case of certain unpublished works of unknown authorship]

(1) In order that the author of a literary or artistic work protected by this Convention shall, in the absence of proof to the contrary, be regarded as such, and consequently be entitled to institute infringement proceedings in the countries of the Union, it shall be sufficient for his name to appear on the work in the usual manner. This paragraph shall be applicable even if this name is a pseudonym, where the pseudonym adopted by the author leaves no doubt as to his identity.

(2) The person or body corporate whose name appears on a cinematographic work in the usual manner shall, in the absence of proof to the contrary, be presumed to be the maker of the said work.

(3) In the case of anonymous and pseudonymous works, other than those referred to in paragraph (1) above, the publisher whose name appears on the work shall, in the absence of proof to the contrary, be deemed to represent the author, and in this capacity he shall be entitled to protect and enforce the author's rights. The provisions of this paragraph shall cease to apply when the author reveals his identity and establishes his claim to authorship of the work.

(4) (a) In the case of unpublished works where the identity of the author is unknown, but where there is every ground to presume that he is a national of a country of the Union, it shall be a matter for legislation in that country to designate the competent authority which shall represent the author and shall be entitled to protect and enforce his rights in the countries of the Union.

(b) Countries of the Union which make such designation under the terms of this provision shall notify the Director General by means of a written declaration giving full information concerning the authority thus designated. The Director General shall at once communicate this declaration to all other countries of the Union.

Article 16
[Infringing Copies: 1. Seizure; 2. Seizure on importation; 3. Applicable law]

(1) Infringing copies of a work shall be liable to seizure in any country of the Union where the work enjoys legal protection.

(2) The provisions of the preceding paragraph shall also apply to reproductions coming from a country where the work is not protected, or has ceased to be protected.

(3) The seizure shall take place in accordance with the legislation of each country.

Article 17
[Possibility of Control of Circulation, Presentation and Exhibition of Works]

The provisions of this Convention cannot in any way affect the right of the Government of each country of the Union to permit, to control, or to prohibit, by legislation or regulation, the circulation, presentation, or exhibition of any work or production in regard to which the competent authority may find it necessary to exercise that right.

Article 18
[Works Existing on Convention's Entry Into Force: 1. Protectable where protection not yet expired in country of origin; 2. Non-protectable where protection already expired in country where it is claimed; 3. Application of these principles; 4. Special cases]

(1) This Convention shall apply to all works which, at the moment of its coming into force, have not yet fallen into the public domain in the country of origin through the expiry of the term of protection.

(2) If, however, through the expiry of the term of protection which was previously granted, a work has fallen into the public domain in the country of origin where protection is claimed, that work shall not be protected anew.

(3) The application of this principle shall be subject to any provisions contained in special conventions to that effect entering into force or to be concluded between countries of the Union. In the absence of such provisions, the respective countries shall determine, each in so far as it is concerned, the conditions of application of this principle.

(4) The preceding provisions shall also apply in the case of new accessions to the Union and to cases in which protection is extended by the application of Article 7 or by the abandonment of reservations.

Article 19
[Protection Greater than Resulting from Convention]

The provisions of this Convention shall not preclude the making of a claim to the benefit of any greater protection which may be granted by legislation in a country of the Union.

Article 20
[Special Agreements Among Countries of the Union]

The Governments of the countries of the Union reserve the right to enter into special agreements among themselves, in so far as such agreements grant to authors more extensive rights than those granted by the Convention, or contain other provisions not contrary to this Convention. The provisions of existing agreements which satisfy these conditions shall remain applicable.

Article 21
[Special Provisions Regarding Developing Countries: 1. Reference to Appendix; 2. Appendix part of Act]

(1) Special provisions regarding developing countries are included in the Appendix.

(2) Subject to the provisions of Article 28(1)(b), the Appendix forms an integral part of this Act.
Article 24


(1) (a) The administrative tasks with respect to the Union shall be performed by the International Bureau, which is a continuation of the Bureau of the Union united with the Bureau of the Union established by the International Convention for the Protection of Industrial Property.

(b) In particular, the International Bureau shall provide the secretariat of the various organs of the Union.

(c) The Director General of the Organization shall be the chief executive of the Union and shall represent the Union.

(2) The International Bureau shall assemble and publish information concerning the protection of copyright. Each country of the Union shall promptly communicate to the International Bureau all new laws and official texts concerning the protection of copyright.

(3) The International Bureau shall publish a monthly periodical.

(4) The International Bureau shall, on request, furnish information to any country of the Union on matters concerning the protection of copyright.

(5) The International Bureau shall conduct studies, and shall provide services, designed to facilitate the protection of copyright.

(6) The Director General and any staff member designated by him shall participate, without the right to vote, in all meetings of the Assembly, the Executive Committee and any other committee of experts or working group. The Director General, or a staff member designated by him, shall be ex officio secretary of these bodies.

(7) (a) The International Bureau shall, in accordance with the directions of the Assembly and in cooperation with the Executive Committee, make the preparations for the conferences of revision of the provisions of the Convention other than Article 22 to Article 26.

(b) The International Bureau may consult with intergovernmental and international non-governmental organizations concerning preparations for conferences of revision.

(c) The Director General and persons designated by him shall take part, without the right to vote, in the discussions at these conferences.

(8) The International Bureau shall carry out any other tasks assigned to it.

[...]

Article 26

[Amendments: 1. Provisions susceptible of amendment by the Assembly; proposals; 2. Adoption; 3. Entry into force]

(1) Proposals for the amendment of Article 22, Article 23, Article 24, Article 25, and the present Article, may be initiated by any country member of the Assembly, by the Executive Committee, or by the Director General. Such proposals shall be communicated by the Director General to the member countries of the Assembly at least six months in advance of their consideration by the Assembly.

(2) Amendments to the Articles referred to in paragraph (1) shall be adopted by the Assembly. Adoption shall require three-fourths of the votes cast, provided that any amendment of Article 22, and of the present paragraph, shall require four-fifths of the votes cast.

(3) Any amendment to the Articles referred to in paragraph (1) shall enter into force one month after written notifications of acceptance, effected in accordance with their respective constitutional processes, have been received by the Director General from three-fourths of the countries members of the Assembly at the time it adopted the amendment. Any amendment to the said Articles thus accepted shall bind all the countries which are members of the Assembly at the time the amendment enters into force, or which become members thereof at a subsequent date, provided that any amendment increasing the financial obligations of countries of the Union shall bind only those countries which have notified their acceptance of such amendment.

Article 27

[Revision: 1. Objective; 2. Conferences; 3. Adoption]

(1) This Convention shall be submitted to revision with a view to the introduction of amendments designed to improve the system of the Union.

(2) For this purpose, conferences shall be held successively in one of the countries of the Union among the delegates of the said countries.

(3) Subject to the provisions of Article 26 which apply to the amendment of Article 22 to Article 26, any revision of this Act, including the Appendix, shall require the unanimity of the votes cast.

Article 28

[Acceptance and Entry Into Force of Act for Countries of the Union: 1. Ratification, accession; possibility of excluding certain provisions; withdrawal of exclusion; 2. Entry into force of Articles 1 to 21 and Appendix; 3. Entry into force of Articles 22 to 38]

(1) (a) Any country of the Union which has signed this Act may ratify it, and, if it has not signed it, may accede to it. Instruments of ratification or accession shall be deposited with the Director General.

(b) Any country of the Union may declare in its instrument of ratification or accession that its ratification or accession shall not apply to Article 1 to Article 21 and the Appendix, provided that, if such country has previously made a declaration under Article VII(1) of the Appendix, then it may declare in the said instrument only that its ratification or accession shall not apply to Article 1 to Article 20.

(c) Any country of the Union which, in accordance with subparagraph (b), has excluded provisions therein referred to from the effects of its ratification or accession may at any later time declare that it extends the effects of its ratification or accession to those provisions. Such declaration shall be deposited with the Director General.

(2) (a) Article 1 to Article 21 and the Appendix shall enter into force three months after both of the following two conditions are fulfilled:

(i) at least five countries of the Union have ratified or acceded to this Act without making a declaration under paragraph (1)(b).

(ii) France, Spain, the United Kingdom of Great Britain and Northern Ireland, and the United States of America, have become bound by the Universal Copyright Convention as revised at Paris on July 24, 1971.

(b) The entry into force referred to in subparagraph (a) shall apply to those countries of the Union which, at least three months before the said entry into force, have deposited instruments of ratification or accession not containing a declaration under paragraph (1)(b).

(c) With respect to any country of the Union not covered by subparagraph (b) and which ratifies or accedes to this Act without making a declaration under paragraph (1)(b), Article 1 to Article 21 and the Appendix shall enter into force three months after the date on which the Director General has notified the deposit of the relevant instrument of ratification or accession, unless a subsequent date has been indicated in the instrument deposited. In the latter case, Article 1 to Article 21 and the Appendix shall enter into force with respect to that country on the date thus indicated.
Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations

The Contracting States, moved by the desire to protect the rights of performers, producers of phonograms, and broadcasting organisations, have agreed as follows:

Article 1 Safeguard of Copyright Proper
Protection granted under this Convention shall leave intact and shall in no way affect the protection of copyright in literary and artistic works. Consequently, no provision of this Convention may be interpreted as prejudicing such protection.

Article 2 Protection given by the Convention.
Definition of National Treatment
1. For the purposes of this Convention, national treatment shall mean the treatment accorded by the domestic law of the Contracting State in which protection is claimed:
(a) to performers who are its nationals, as regards performances taking place, broadcast, or first fixed, on its territory;
(b) to producers of phonograms who are its nationals, as regards phonograms first fixed or first published on its territory;
(c) to broadcasting organisations which have their headquarters on its territory, as regards broadcasts transmitted from transmitters situated on its territory.
2. National treatment shall be subject to the protection specifically guaranteed, and the limitations specifically provided for, in this Convention.

Article 3 Definitions:
(a) Performers;
(b) Phonogram;
(c) Producers of Phonograms;
(d) Publication;
(e) Reproduction;
(f) Broadcasting;
(g) Rebroadcasting
For the purposes of this Convention:
(a) "performers" means actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, or otherwise perform literary or artistic works;
(b) "phonogram" means any exclusively aural fixation of sounds of a performance or of other sounds;
(c) "producer of phonograms" means the person who, or the legal entity which, first fixes the sounds of a performance or other sounds;
(d) "publication" means the offering of copies of a phonogram to the public in reasonable quantity;
(e) "reproduction" means the making of a copy or copies of a fixation;
(f) "broadcasting" means the transmission by wireless means for public reception of sounds or of images and sounds;
(g) "rebroadcasting" means the simultaneous broadcasting by one broadcasting organisation of the broadcast of another broadcasting organisation.

Article 4 Performances Protected.
Points of Attachment for Performers
Each Contracting State shall grant national treatment to performers if any of the following conditions is met:
(a) the performance takes place in another Contracting State;
(b) the performance is incorporated in a phonogram which is protected under Article 5 of this Convention;
(c) the performance, not being fixed on a phonogram, is carried by a broadcast which is protected by Article 6 of this Convention.

Article 5 Protected Phonograms: 1. Points of Attachment for Producers of Phonograms;
2. Simultaneous Publication; 3. Power to exclude certain Criteria
1. Each Contracting State shall grant national treatment to producers of phonograms if any of the following conditions is met:
(a) the producer of the phonogram is a national of another Contracting State (criterion of nationality);
(b) the first fixation of the sound was made in another Contracting State (criterion of fixation);
(c) the phonogram was first published in another Contracting State (criterion of publication).
2. If a phonogram was first published in a non-Contracting State but if it was also published, within thirty days of its first publication, in a Contracting State (simultaneous publication), it shall be considered as first published in the Contracting State.
3. By means of a notification deposited with the Secretary-General of the United Nations, any Contracting State may declare that it will not apply the criterion of publication or, alternatively, the criterion of fixation. Such notification may be deposited at the time of ratification, acceptance or accession, or at any time thereafter; in the last case, it shall become effective six months after it has been deposited.

Article 6 Protected Broadcasts: 1. Points of Attachment for Broadcasting Organizations; 2. Power to Reserve
1. Each Contracting State shall grant national treatment to broadcasting organisations if either of the following conditions is met:
(a) the headquarters of the broadcasting organisation is situated in another Contracting State;
(b) the broadcast was transmitted from a transmitter situated in another Contracting State.
2. By means of a notification deposited with the Secretary-General of the United Nations, any Contracting State may declare that it will protect broadcasts only if the headquarters of the broadcasting organisation is situated in another Contracting State and the broadcast was transmitted from a transmitter situated in the same Contracting State. Such notification may be deposited at the time of ratification,
Article 7
Minimum Protection for Performers: 1. Particular Rights; 2. Relations between Performers and Broadcasting Organizations

1. The protection provided for performers by this Convention shall include the possibility of preventing:
   (a) the broadcasting and the communication to the public, without their consent, of their performance, except where the performance used in the broadcasting or the public communication is itself already a broadcast performance or is made from a fixation;
   (b) the fixation, without their consent, of their unfixed performance;
   (c) the reproduction, without their consent, of a fixation of their performance:
      (i) if the original fixation itself was made without their consent;
      (ii) if the reproduction is made for purposes different from those for which the performers gave their consent;
      (iii) if the original fixation was made in accordance with the provisions of Article 15, and the reproduction is made for purposes different from those referred to in those provisions.

2. (1) If broadcasting was consented to by the performers, it shall be a matter for the domestic law of the Contracting State where protection is claimed to regulate the protection against rebroadcasting, fixation for broadcasting purposes and the reproduction of such fixation for broadcasting purposes.
   (2) The terms and conditions governing the use by broadcasting organisations of fixations made for broadcasting purposes shall be determined in accordance with the domestic law of the Contracting State where protection is claimed.
   (3) However, the domestic law referred to in sub-paragraphs (1) and (2) of this paragraph shall not operate to deprive performers of the ability to control, by contract, their relations with broadcasting organisations.

Article 8
Performers acting jointly
Any Contracting State may, by its domestic laws and regulations, specify the manner in which performers will be represented in connection with the exercise of their rights if several of them participate in the same performance.

Article 9
Variety and Circus Artists
Any Contracting State may, by its domestic laws and regulations, extend the protection provided for in this Convention to artists who do not perform literary or artistic works.

Article 10
Right of Reproduction for Phonogram Producers
Producers of phonograms shall enjoy the right to authorize or prohibit the direct or indirect reproduction of their phonograms.

Article 11
Formalities for Phonograms
If, as a condition of protecting the rights of producers of phonograms, or of performers, or both, in relation to phonograms, a Contracting State, under its domestic law, requires compliance with formalities, these shall be considered as fulfilled if all the copies in commerce of the published phonogram or their containers bear a notice consisting of the symbol (P), accompanied by the year date of the first publication, placed in such a manner as to give reasonable notice of claim of protection; and if the copies or their containers do not identify the producer or the licensee of the producer (by carrying his name, trade mark or other appropriate designation), the notice shall also include the name of the owner of the rights of the producer; and, furthermore, if the copies or their containers do not identify the principal performers, the notice shall also include the name of the person who, in the country in which the fixation was effected, owns the rights of such performers.

Article 12
Secondary Uses of Phonograms
If a phonogram published for commercial purposes, or a reproduction of such phonogram, is used directly for broadcasting or for any communication to the public, a single equitable remuneration shall be paid by the user to the performers, or to the producers of the phonograms, or to both. Domestic law may, in the absence of agreement between these parties, lay down the conditions as to the sharing of this remuneration.

Article 13
Minimum Rights for Broadcasting Organizations
Broadcasting organisations shall enjoy the right to authorize or prohibit:
   (a) the rebroadcasting of their broadcasts;
   (b) the fixation of their broadcasts;
   (c) the reproduction:
      (i) of fixations, made without their consent, of their broadcasts;
      (ii) of fixations, made in accordance with the provisions of Article 15, of their broadcasts, if the reproduction is made for purposes different from those referred to in those provisions;
      (iii) of the communication to the public of their television broadcasts if such communication is made in places accessible to the public against payment of an entrance fee; it shall be a matter for the domestic law of the State where protection of this right is claimed to determine the conditions under which it may be exercised.

Article 14
Minimum Duration of Protection
The term of protection to be granted under this Convention shall last at least until the end of a period of twenty years computed from the end of the year in which:
   (a) the fixation was made for phonograms and for performances incorporated therein;
   (b) the performance took place for performances not incorporated in phonograms;
   (c) the broadcast took place for broadcasts.

Article 15
Permitted Exceptions: 1. Specific Limitations; 2. Equivalents with copyright
1. Any Contracting State may, in its domestic laws and regulations, provide for exceptions to the protection guaranteed by this Convention as regards:
   (a) private use;
   (b) use of short excerpts in connection with the reporting of current events;
   (c) ephemeral fixation by a broadcasting organisation by means of its own facilities and for its own broadcasts;
   (d) use solely for the purposes of teaching or scientific research.
2. Irrespective of paragraph 1 of this Article, any Contracting State may, in its domestic laws and regulations, provide for the same kinds of limitations with regard to the protection of performers, producers of phonograms and broadcasting organisations, as it provides for, in its domestic laws and regulations, in connection with the protection of copyright in literary and artistic works. However, compulsory licences may be provided for only to the extent to which they are compatible with this Convention.
Article 16
Reservations
1. Any State, upon becoming party to this Convention, shall be bound by all the obligations and shall enjoy all the benefits thereof. However, a State may at any time, in a notification deposited with the Secretary-General of the United Nations, declare that:

(a) as regards Article 12:
(i) it will not apply the provisions of that Article;
(ii) it will not apply the provisions of that Article in respect of certain uses;
(iii) as regards phonograms the producer of which is not a national of another Contracting State, it will not apply that Article;
(iv) as regards phonograms the producer of which is a national of another Contracting State, it will limit the protection provided for by that Article to the extent to which, and to the term for which, the latter State grants protection to phonograms first fixed by a national of the State making the declaration; however, the fact that the Contracting State of which the producer is a national does not grant the protection to the same beneficiary or beneficiaries as the State making the declaration shall not be considered as a difference in the extent of the protection;
(b) as regards Article 13, it will not apply the provisions of that Article; if a Contracting State makes such a declaration, the other Contracting States shall not be obliged to grant the right referred to in Article 13, item (d), to broadcasting organisations whose headquarters are in that State.
2. If the notification referred to in paragraph 1 of this Article is made after the date of the deposit of the instrument of ratification, acceptance or accession, the declaration will become effective six months after it has been deposited.

Article 17
Certain countries applying only the “fixation” criterion
Any State which, on October 26, 1961, grants protection to producers of phonograms solely on the basis of the criterion of fixation may, by a notification deposited with the Secretary-General of the United Nations at the time of ratification, acceptance or accession, declare that it will apply, for the purposes of Article 5, the criterion of fixation alone and, for the purposes of paragraph 1(e)(ii) and (iv) of Article 16, the criterion of fixation instead of the criterion of nationality.

Article 18
Withdrawal of reservations
Any State which has deposited a notification under paragraph 3 of Article 5, paragraph 2 of Article 6, paragraph 1 of Article 16 or Article 17, may, by a further notification deposited with the Secretary-General of the United Nations, reduce its scope or withdraw it.

Article 19
Performers’ Rights in Films
Notwithstanding anything in this Convention, once a performer has consented to the incorporation of his performance in a visual or audio-visual fixation, Article 7 shall have no further application.

Article 20
Non-retroactivity
1. This Convention shall not prejudice rights acquired in any Contracting State before the date of coming into force of this Convention for that State.
2. No Contracting State shall be bound to apply the provisions of this Convention to performances or broadcasts which took place, or to phonograms which were fixed, before the date of coming into force of this Convention for that State.

Article 21
Protection by other means
The protection provided for in this Convention shall not prejudice any protection otherwise secured to performers, producers of phonograms and broadcasting organisations.

Article 22
Special agreements
Contracting States reserve the right to enter into special agreements among themselves in so far as such agreements grant to performers, producers of phonograms or broadcasting organisations more extensive rights than those granted by this Convention or contain other provisions not contrary to this Convention.

Article 23
Signature and deposit
This Convention shall be deposited with the Secretary-General of the United Nations. It shall be open until June 30, 1962, for signature by any State invited to the Diplomatic Conference on the International Protection of Performers, Producers of Phonograms and Broadcasting Organisations which is a party to the Universal Copyright Convention or a member of the International Union for the Protection of Literary and Artistic Works.

Article 24
Becoming Party to the Convention
1. This Convention shall be subject to ratification or acceptance by any State.
2. This Convention shall be open for accession by any State at the Conference referred to in Article 23, and by any State Member of the United Nations, provided that in either case such State is a party to the Universal Copyright Convention or a member of the International Union for the Protection of Literary and Artistic Works.
3. Ratification, acceptance or accession shall be effected by deposit of an instrument to that effect with the Secretary-General of the United Nations.

[...]

Article 26
Implementation of the Convention by the Provision of Domestic Law
1. Each Contracting State undertakes to adopt, in accordance with its Constitution, the measures necessary to ensure the application of this Convention.
2. At the time of deposit of its instrument of ratification, acceptance or accession, each State must be in a position under its domestic law to give effect to the terms of this Convention.

Article 27
Applicability of the Convention to Certain Territories
1. Any State may, at the time of ratification, acceptance or accession, or at any time thereafter, declare by notification addressed to the Secretary-General of the United Nations that this Convention shall extend to all or any of the territories for whose international relations it is responsible, provided that the Universal Copyright Convention or the International Convention for the Protection of Literary and Artistic Works applies to the territory or territories concerned. This notification shall take effect three months after the date of its receipt.
2. The notifications referred to in paragraph 3 of Article 5, paragraph 2 of Article 6, paragraph 1 of Article 16 and Articles 17 and 18, may be extended to cover all or any of the territories referred to in paragraph 1 of this Article.

Article 28
Denunciation of the Convention
Article 29
Revision of the Convention
1. After this Convention has been in force for five years, any Contracting State may, by notification addressed to the Secretary-General of the United Nations, request that a conference be convened for the purpose of revising the Convention. The Secretary-General shall notify all Contracting States of this request. If within a period of six months following the date of notification by the Secretary-General of the United Nations, not less than one half of the Contracting States notify him of their concurrence with the request, the Secretary-General shall inform the Director-General of the International Labor Office, the Director-General of the United Nations Educational, Scientific and Cultural Organization and the Director of the Bureau of the International Union for the Protection of Literary and Artistic Works, who shall convene a revision conference in cooperation with the Intergovernmental Committee provided for in Article 32.
2. The adoption of any revision of this Convention shall require an affirmative vote by two-thirds of the States attending the revision conference, provided that this majority includes two-thirds of the States which, at the time of the revision conference, are parties to the Convention.
3. In the event of adoption of a Convention revising this Convention in whole or in part, and unless the revising Convention provides otherwise:
   (a) this Convention shall cease to be open to ratification, acceptance or accession from the date of entry into force of the revising Convention;
   (b) this Convention shall remain in force as regards relations between or with Contracting States which have not become parties to the revising Convention.

Article 30
Settlement of disputes
Any dispute which may arise between two or more Contracting States concerning the interpretation or application of this Convention and which is not settled by negotiation shall, at the request of any one of the parties to the dispute, be referred to the International Court of Justice for decision, unless they agree to another mode of settlement.

Article 31
Limits on Reservations
Without prejudice to the provisions of paragraph 3 of Article 5, paragraph 2 of Article 6, paragraph 1 of Article 16 and Article 17, no reservation may be made to this Convention.

Article 32
Intergovernmental Committee
1. An Intergovernmental Committee is hereby established with the following duties:
   (a) to study questions concerning the application and operation of this Convention; and
   (b) to collect proposals and to prepare documentation for possible revision of this Convention.
2. The Committee shall consist of representatives of the Contracting States, chosen with due regard to equitable geographical distribution. The number of members shall be six if there are twelve Contracting States or less, nine if there are thirteen to eighteen Contracting States and twelve if there are more than eighteen Contracting States.
3. The Committee shall be constituted twelve months after this Convention comes into force by an election organized among the Contracting States, each of which shall have one vote, by the Director-General of the International Labor Office, the Director-General of the United Nations Educational, Scientific and Cultural Organization and the Director of the Bureau of the International Union for the Protection of Literary and Artistic Works, in accordance with rules previously approved by a majority of all Contracting States.
4. The Committee shall elect its Chairman and officers. It shall establish its own rules of procedure. These rules shall in particular provide for the future operation of the Committee and for a method of selecting its members for the future in such a way as to ensure rotation among the various Contracting States.
6. Meetings of the Committee, which shall be convened whenever a majority of its members deems it necessary, shall be held successively at the headquarters of the International Labor Office, the United Nations Educational, Scientific and Cultural Organization, and the Bureau of the International Union for the Protection of Literary and Artistic Works.
7. Expenses of members of the Committee shall be borne by their respective Governments.

Article 33
Languages
1. The present Convention is drawn up in English, French and Spanish, the three texts being equally authentic.
2. In addition, official texts of the present Convention shall be drawn up in German, Italian and Portuguese.

Article 34
Notifications
1. The Secretary-General of the United Nations shall notify the States invited to the Conference referred to in Article 23 and every State Member of the United Nations, as well as the Director-General of the International Labor Office, the Director-General of the United Nations Educational, Scientific and Cultural Organization and the Director of the Bureau of the International Union for the Protection of Literary and Artistic Works:
   (a) of the deposit of each instrument of ratification, acceptance or accession from the date of entry into force of the Convention;
   (b) of the date of entry into force of the Convention;
   (c) of all notifications, declarations or communications provided for in this Convention;
   (d) if any of the situations referred to in paragraphs 4 and 5 of Article 28 arise.

[...]
[...]

Institute of Law and Technology
Masaryk University, Faculty of Law
Preamble

The Contracting Parties, Desiring to develop and maintain the protection of the rights of authors in their literary and artistic works in a manner as effective and uniform as possible,

Recognizing the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by new economic, social, cultural and technological developments,

Recognizing the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works,

Emphasizing the outstanding significance of copyright protection as an incentive for literary and artistic creation,

Recognizing the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention,

Have agreed as follows:

Article 1

Relation to the Berne Convention

(1) This Treaty is a special agreement within the meaning of Article 20 of the Berne Convention for the Protection of Literary and Artistic Works, as regards Contracting Parties that are countries of the Union established by that Convention. This Treaty shall not have any connection with treaties other than the Berne Convention, nor shall it prejudice any rights and obligations under any other treaties.

(2) Nothing in this Treaty shall derogate from existing obligations that Contracting Parties have to each other under the Berne Convention for the Protection of Literary and Artistic Works.


(4) Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention.1

Article 2

Scope of Copyright Protection

Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.

Article 3

Application of Articles 2 to 6 of the Berne Convention

Contracting Parties shall apply mutatis mutandis the provisions of Articles 2 to 6 of the Berne Convention in respect of the protection provided for in this Treaty.2

Article 4

Computer Programs

Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.3

Article 5

Compilations of Data (Databases)

Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation.4

Article 6

Right of Distribution

(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the work with the authorization of the author.5

Article 7

Right of Rental

(1) Authors of

(i) computer programs;

(ii) cinematographic works; and

(iii) works embodied in phonograms, as determined in the national law of Contracting Parties, shall enjoy the exclusive right of authorizing commercial rental to the public of the originals or copies of their works.

(2) Paragraph (1) shall not apply

(i) in the case of computer programs, where the program itself is not the essential object of the rental; and

(ii) in the case of cinematographic works, unless such commercial rental has led to widespread copying of such works materially impairing the exclusive right of reproduction.

(3) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of authors for the rental of copies of their works embodied in phonograms may maintain that system provided that the commercial rental of works embodied in phonograms is not giving rise to the material impairment of the exclusive right of reproduction of authors.6

Article 8

Right of Communication to the Public

Without prejudice to the provisions of Articles 11(1)(i), 11bis(1)(i) and (ii), 11ter(1)(ii), 14(1)(ii) and 14bis(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.7

Article 9

Duration of the Protection of Photographic Works

In respect of photographic works, the Contracting Parties shall not apply the provisions of Article 7(4) of the Berne Convention.

Article 10

Limitations and Exceptions

(1) Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

(2) Contracting Parties shall, when applying the Berne Convention, confine any limitations of or exceptions to rights provided for therein to certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.8
Article 11
Obligations concerning Technological Measures
Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Article 12
Obligations concerning Rights Management Information
(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:
   (i) to remove or alter any electronic rights management information without authority;
   (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.
(2) As used in this Article, “rights management information” means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.9

Article 13
Application in Time
Contracting Parties shall apply the provisions of Article 18 of the Berne Convention to all protection provided for in this Treaty.

Article 14
Provisions on Enforcement of Rights
(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.
(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

Article 15
Assembly
(1)
(a) The Contracting Parties shall have an Assembly.
(b) Each Contracting Party shall be represented by one delegate who may be assisted by alternate delegates, advisors and experts.
(c) The expenses of each delegation shall be borne by the Contracting Party that has appointed the delegation. The Assembly may ask the World Intellectual Property Organization (hereinafter referred to as “WIPO”) to grant financial assistance to facilitate the participation of delegations of Contracting Parties that are regarded as developing countries in conformity with the established practice of the General Assembly of the United Nations or that are countries in transition to a market economy.
(2)
(a) The Assembly shall deal with matters concerning the maintenance and development of this Treaty and the application and operation of this Treaty.
(b) The Assembly shall perform the function allocated to it under Article 17(2) in respect of the admission of certain intergovernmental organizations to become party to this Treaty.
(c) The Assembly shall decide the convocation of any diplomatic conference for the revision of this Treaty and give the necessary instructions to the Director General of WIPO for the preparation of such diplomatic conference.
(3)
(a) Each Contracting Party that is a State shall have one vote and shall vote only in its own name.
(b) Any Contracting Party that is an intergovernmental organization may participate in the vote, in place of its Member States, with a number of votes equal to the number of its Member States which are party to this Treaty. No such intergovernmental organization shall participate in the vote if any one of its Member States exercises its right to vote and vice versa.
(4) The Assembly shall meet in ordinary session once every two years upon convocation by the Director General of WIPO.
(5) The Assembly shall establish its own rules of procedure, including the convocation of extraordinary sessions, the requirements of a quorum and, subject to the provisions of this Treaty, the required majority for various kinds of decisions.

Article 16
International Bureau
The International Bureau of WIPO shall perform the administrative tasks concerning the Treaty.

Article 17
Eligibility for Becoming Party to the Treaty
(1) Any Member State of WIPO may become party to this Treaty.
(2) The Assembly may decide to admit any intergovernmental organization to become party to this Treaty which declares that it is competent in respect of, and has its own legislation binding on all its Member States, matters covered by this Treaty and that it has been duly authorized, in accordance with its internal procedures, to become party to this Treaty.
(3) The European Community, having made the declaration referred to in the preceding paragraph in the Diplomatic Conference that has adopted this Treaty, may become party to this Treaty.

Article 18
Rights and Obligations under the Treaty
Subject to any specific provisions to the contrary in this Treaty, each Contracting Party shall enjoy all of the rights and assume all of the obligations under this Treaty.

Article 19
Signature of the Treaty
This Treaty shall be open for signature until December 31, 1997, by any Member State of WIPO and by the European Community.

Article 20
Entry into Force of the Treaty
This Treaty shall enter into force three months after 30 instruments of ratification or accession by States have been deposited with the Director General of WIPO.

[...]

Article 22
No Reservations to the Treaty
No reservation to this Treaty shall be admitted.

Article 23
Denunciation of the Treaty
This Treaty may be denounced by any Contracting Party by notification addressed to the Director General of WIPO. Any
Article 25
Depositary
The Director General of WIPO is the depositary of this Treaty.

1. Agreed statements concerning Article 1(4): The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.

2. Agreed statements concerning Article 3: It is understood that in applying Article 3 of this Treaty, the expression "country of the Union" in Articles 2 to 6 of the Berne Convention will be read as if it were a reference to a Contracting Party to this Treaty, in the application of those Berne Articles in respect of protection provided for in this Treaty. It is also understood that the expression "country outside the Union" in those Articles in the Berne Convention will, in the same circumstances, be read as if it were a reference to a Contracting Party to this Treaty, and that "this Convention" in Articles 2(8), 2bis(2), 3, 4 and 5 of the Berne Convention will be read as if it were a reference to the Berne Convention and this Treaty. Finally, it is understood that a reference in Articles 3 to 6 of the Berne Convention to a "national of one of the countries of the Union" will, when those Articles are applied to this Treaty, mean, in regard to an intergovernmental organization that is a Contracting Party to this Treaty, a national of one of the countries that is member of that organization.

3. Agreed statements concerning Article 4: The scope of protection for computer programs under Article 4 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.

4. Agreed statements concerning Article 5: The scope of protection for compilations of data (databases) under Article 5 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.

5. Agreed statements concerning Articles 6 and 7: As used in these Articles, the expressions "copies" and "originals and copies," being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects.

6. Agreed statements concerning Article 7: It is understood that the obligation under Article 7(1) does not require a Contracting Party to provide an exclusive right of commercial rental to authors who, under that Contracting Party's law, are not granted rights in respect of phonograms. It is understood that this obligation is consistent with Article 14(4) of the TRIPS Agreement.

7. Agreed statements concerning Article 8: It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11bis(2).

8. Agreed statement concerning Article 10: It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital network environment.

9. Agreed statements concerning Article 12: It is understood that the reference to "infringement of any right covered by this Treaty or the Berne Convention" includes both exclusive rights and rights of remuneration.

It is further understood that Contracting Parties will not rely on this Article to devise or implement rights management systems that would have the effect of imposing formalities which are not permitted under the Berne Convention or this Treaty, prohibiting the free movement of goods or impeding the enjoyment of rights under this Treaty.

WIPO Performances and Phonograms Treaty

Preamble
The Contracting Parties,

Desiring to develop and maintain the protection of the rights of performers and producers of phonograms in a manner as effective and uniform as possible,

Recognizing the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments,

Recognizing the profound impact of the development and convergence of information and communication technologies on the production and use of performances and phonograms,

Recognizing the need to maintain a balance between the rights of performers and producers of phonograms and the larger public interest, particularly education, research and access to information,

Have agreed as follows:

CHAPTER I
General Provisions

Article 1
Relation to Other Conventions

(1) Nothing in this Treaty shall derogate from existing obligations that Contracting Parties have to each other under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations done in Rome, October 26, 1961 (hereinafter the "Rome Convention").

(2) Protection granted under this Treaty shall leave intact and shall in no way affect the protection of copyright in literary and artistic works. Consequently, no provision of this Treaty may be interpreted as prejudicing such protection.

(3) This Treaty shall not have any connection with, nor shall it prejudice any rights and obligations under, any other treaties.
For the purposes of this Treaty:

(a) "performers" are actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret, or otherwise perform literary or artistic works or expressions of folklore;

(b) "phonogram" means the fixation of the sounds of a performance or of other sounds, or of a representation of sounds, other than in the form of a fixation incorporated in a cinematographic or other audiovisual work;

(c) "fixation" means the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device;

(d) "producer of a phonogram" means the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds;

(e) "publication" of a fixed performance or a phonogram means the offering of copies of the fixed performance or the phonogram to the public, with the consent of the rightholder, and provided that copies are offered to the public in reasonable quantity;

(f) "broadcasting" means the transmission by wireless means for public reception of sounds or of images and sounds or of the representations thereof; such transmission by satellite is also "broadcasting"; transmission of encrypted signals is "broadcasting" where the means for decrypting are provided to the public by the broadcasting organization or with its consent;

(g) "communication to the public" of a performance or a phonogram means the transmission to the public by any medium, otherwise than by broadcasting, of sounds or other sounds or of the representations of sounds fixed in a phonogram. For the purposes of Article 15, "communication to the public" includes making the sounds or representations of sounds fixed in a phonogram audible to the public.

Article 3  Beneficiaries of Protection under this Treaty

(1) Contracting Parties shall accord the protection provided under this Treaty to the performers and producers of phonograms who are nationals of other Contracting Parties.

(2) The nationals of other Contracting Parties shall be understood to be those performers or producers of phonograms who would meet the criteria for eligibility for protection as provided under the Rome Convention, were all the Contracting Parties to this Treaty Contracting States of that Convention. In respect of these criteria of eligibility, Contracting Parties shall apply the relevant definitions in Article 2 of this Treaty.

(3) Any Contracting Party availing itself of the possibilities provided in Article 5(3) of the Rome Convention or, for the purposes of Article 5 of the same Convention, Article 17 thereof shall make a notification as foreseen in those provisions to the Director General of the World Intellectual Property Organization (WIPO).5

Article 4  National Treatment

(1) Each Contracting Party shall accord to nationals of other Contracting Parties, as defined in Article 3(2), the treatment it accords to its own nationals with regard to the exclusive rights specifically granted in this Treaty, and to the right to equitable remuneration provided for in Article 15 of this Treaty.

(2) The obligation provided for in paragraph (1) does not apply to the extent that another Contracting Party makes use of the reservations permitted by Article 15(3) of this Treaty.

CHAPTER II  Rights of Performers

Article 5  Moral Rights of Performers

(1) Independently of a performer's economic rights, and even after the transfer of those rights, the performer shall, as regards his live aural performances or performances fixed in phonograms, have the right to claim to be identified as the performer of his performances, except where omission is dictated by the manner of the use of the performance, and to object to any distortion, mutilation or other modification of his performances that would be prejudicial to his reputation.

(2) The rights granted to a performer in accordance with paragraph (1) shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the Contracting Party where protection is claimed. However, those Contracting Parties whose legislation, at the moment of their ratification of or accession to this Treaty, does not provide for protection after the death of the performer of all rights set out in the preceding paragraph may provide that some of these rights will, after his death, cease to be maintained.

(3) The means of redress for safeguarding the rights granted under this Article shall be governed by the legislation of the Contracting Party where protection is claimed.

Article 6  Economic Rights of Performers in their Unfixed Performances

Performers shall enjoy the exclusive right of authorizing, as regards their performances:

(i) the broadcasting and communication to the public of their unfixed performances except where the performance is already a broadcast performance; and

(ii) the fixation of their unfixed performances.

Article 7  Right of Reproduction

Performers shall enjoy the exclusive right of authorizing the direct or indirect reproduction of their performances fixed in phonograms, in any manner or form.

Article 8  Right of Distribution

(1) Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the fixed performance with the authorization of the performer.

Article 9  Right of Rental

(1) Performers shall enjoy the exclusive right of authorizing the commercial rental to the public of the original and copies of their performances fixed in phonograms as determined in the national law of Contracting Parties, even after distribution of them by, or pursuant to, authorization by the performer.

(2) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of performers for the rental of copies of their performances fixed...
in phonograms, may maintain that system provided that the commercial rental of phonograms is not giving rise to the material impairment of the exclusive right of reproduction of performers.8

Article 10
Right of Making Available of Fixed Performances

Performers shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

CHAPTER III
Rights of Producers of Phonograms

Article 11
Right of Reproduction

Producers of phonograms shall enjoy the exclusive right of authorizing the direct or indirect reproduction of their phonograms, in any manner or form.9

Article 12
Right of Distribution

(1) Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their phonograms through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the phonogram with the authorization of the producer of the phonogram.10

Article 13
Right of Rental

(1) Producers of phonograms shall enjoy the exclusive right of authorizing the commercial rental to the public of the original and copies of their phonograms, even after distribution of them, by or pursuant to, authorization by the producer.

(2) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of producers of phonograms for the rental of copies of their phonograms, may maintain that system provided that the commercial rental of phonograms is not giving rise to the material impairment of the exclusive rights of reproduction of producers of phonograms.11

Article 14
Right of Making Available of Phonograms

Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

CHAPTER IV
Common Provisions

Article 15
Right to Remuneration for Broadcasting and Communication to the Public

(1) Performers and producers of phonograms shall enjoy the right to a single equitable remuneration for the direct or indirect use of phonograms published for commercial purposes for broadcasting or for any communication to the public.

(2) Contracting Parties may establish in their national legislation that the single equitable remuneration shall be claimed from the user by the performer or by the producer of a phonogram or by both. Contracting Parties may enact national legislation that, in the absence of an agreement between the performer and the producer of a phonogram, sets the terms according to which performers and producers of phonograms shall share the single equitable remuneration.

(3) Any Contracting Party may, in a notification deposited with the Director General of WIPO, declare that it will apply the provisions of paragraph (1) only in respect of certain uses, or that it will limit their application in some other way, or that it will not apply these provisions at all.

(4) For the purposes of this Article, phonograms made available to the public by wire or wireless means in such a way that members of the public may access them from a place and at a time individually chosen by them shall be considered as if they had been published for commercial purposes.12,13

Article 16
Limitations and Exceptions

(1) Contracting Parties may, in their national legislation, provide for the same kinds of limitations or exceptions with regard to the protection of performers and producers of phonograms as they provide for, in their national legislation, in connection with the protection of copyright in literary and artistic works.

(2) Contracting Parties shall confine any limitations of or exceptions to rights provided for in this Treaty to certain special cases which do not conflict with a normal exploitation of the performance or phonogram and do not unreasonably prejudice the legitimate interests of the performer or of the producer of the phonogram.14,15

Article 17
Term of Protection

(1) The term of protection to be granted to performers under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the performance was fixed in a phonogram.

(2) The term of protection to be granted to producers of phonograms under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the phonogram was published, or failing such publication within 50 years from fixation of the phonogram, 50 years from the end of the year in which the fixation was made.

Article 18
Obligations concerning Technological Measures

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.

Article 19
Obligations concerning Rights Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty.
(i) to remove or alter any electronic rights management information without authority;
(ii) to distribute, import for distribution, broadcast, communicate or make available to the public, without authority, performances, copies of fixed performances or phonograms knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, “rights management information” means information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication or making available of a fixed performance or a phonogram to the public.\textsuperscript{16}

\textbf{Article 20}

\textbf{Formalities}

The enjoyment and exercise of the rights provided for in this Treaty shall not be subject to any formality.

\textbf{Article 21}

\textbf{Reservations}

Subject to the provisions of Article 15(3), no reservations to this Treaty shall be permitted.

\textbf{Article 22}

\textbf{Application in Time}

(1) Contracting Parties shall apply the provisions of Article 18 of the Berne Convention, mutatis mutandis, to the rights of performers and producers of phonograms provided for in this Treaty.

(2) Notwithstanding paragraph (1), a Contracting Party may limit the application of Article 5 of this Treaty to performances which occurred after the entry into force of this Treaty for that Party.

\textbf{Article 23}

\textbf{Provisions on Enforcement of Rights}

(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

\textbf{CHAPTER V}

\textbf{Administrative and Final Clauses}

\textbf{Article 24}

\textbf{Assembly}

(1) (a) The Contracting Parties shall have an Assembly.

(b) Each Contracting Party shall be represented by one delegate who may be assisted by alternate delegates, advisors and experts.

(c) The expenses of each delegation shall be borne by the Contracting Party that has appointed the delegation. The Assembly may ask WIPO to grant financial assistance to facilitate the participation of delegations of Contracting Parties that are regarded as developing countries in conformity with the established practice of the General Assembly of the United Nations or that are countries in transition to a market economy.

(2) (a) The Assembly shall deal with matters concerning the maintenance and development of this Treaty and the application and operation of this Treaty.

(b) The Assembly shall perform the function allocated to it under Article 26(2) in respect of the admission of certain intergovernmental organizations to become party to this Treaty.

(c) The Assembly shall decide the convocation of any diplomatic conference for the revision of this Treaty and give the necessary instructions to the Director General of WIPO for the preparation of such diplomatic conference.

(3) (a) Each Contracting Party that is a State shall have one vote and shall vote only in its own name.

(b) Any Contracting Party that is an intergovernmental organization may participate in the vote, in place of its Member States, with a number of votes equal to the number of its Member States which are party to this Treaty. No such intergovernmental organization shall participate in the vote if any one of its Member States exercises its right to vote and vice versa.

(4) The Assembly shall meet in ordinary session once every two years upon convocation by the Director General of WIPO.

(5) The Assembly shall establish its own rules of procedure, including the convocation of extraordinary sessions, the requirements of a quorum and, subject to the provisions of this Treaty, the required majority for various kinds of decisions.

\textbf{Article 25}

\textbf{International Bureau}

The International Bureau of WIPO shall perform the administrative tasks concerning the Treaty.

\textbf{Article 26}

\textbf{Eligibility for Becoming Party to the Treaty}

(1) Any Member State of WIPO may become party to this Treaty.

(2) The Assembly may decide to admit any intergovernmental organization to become party to this Treaty which declares that it is competent in respect of, and has its own legislation binding on all its Member States on, matters covered by this Treaty and that it has been duly authorized, in accordance with its internal procedures, to become party to this Treaty.

(3) The European Community, having made the declaration referred to in the preceding paragraph in the Diplomatic Conference that has adopted this Treaty, may become party to this Treaty.

\textbf{Article 27}

\textbf{Rights and Obligations under the Treaty}

Subject to any specific provisions to the contrary in this Treaty, each Contracting Party shall enjoy all of the rights and assume all of the obligations under this Treaty.

\[\]

\textbf{Article 31}

\textbf{Denunciation of the Treaty}

This Treaty may be denounced by any Contracting Party by notification addressed to the Director General of WIPO. Any denunciation shall take effect one year from the date on which the Director General of WIPO received the notification.

[...]

(1) The Treaty provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. Harmonisation of the laws of the Member States on copyright and related rights contributes to the achievement of these objectives.

(2) The European Council, meeting at Corfu on 24 and 25 June 1994, stressed the need to create a general and flexible legal framework at Community level in order to foster the development of the information society in Europe. This requires, inter alia, the existence of an internal market for new products and services. Important Community legislation to ensure such a regulatory framework is already in place or its adoption is well under way. Copyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content.

(3) The proposed harmonisation will help to implement the four freedoms of the internal market and relates to compliance with the fundamental principles of law and especially of property, including intellectual property, and freedom of expression and the public interest.

(4) A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.

(5) Technological development has multiplied and diversified the vectors for creation, production and exploitation. While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation.

(6) Without harmonisation at Community level, legislative activities at national level which have already been initiated in a number of Member States in order to respond to the technological challenges might result in significant differences in protection and thereby in restrictions on the free movement of services and products incorporating, or based on, intellectual property, leading to a refragmentation of the internal market and legislative inconsistency. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased transborder exploitation of intellectual property. This development will and should further increase. Significant legal differences and uncertainties in protection may hinder economies of scale for new products and services containing copyright and related rights.

(7) The Community legal framework for the protection of copyright and related rights must, therefore, also be adapted and supplemented as far as is necessary for the smooth functioning of the internal market. To that end, those national provisions on copyright and related rights which vary considerably from one Member State to another or which cause legal uncertainties hindering the smooth functioning of the internal market and the proper development of the information society in Europe should be adjusted, and inconsistent national responses to the technological developments should be avoided, whilst differences not adversely affecting the functioning of the internal market need not be removed or prevented.

(8) The various social, societal and cultural implications of the information society require that account be taken of the specific features of the content of products and services.

(9) Any harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognised as an integral part of property.

(10) If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. The investment required to produce products such as phonograms, films or multimedia products, and services such as "on-demand" services, is considerable. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment.

(11) A rigorous, effective system for the protection of copyright and related rights is one of the main ways of ensuring that European cultural creativity and production receive the necessary resources and of safeguarding the independence and dignity of artistic creators and performers.

(12) Adequate protection of copyright works and subject-matter of related rights is also of great importance from a cultural standpoint. Article 151 of the Treaty requires the Community to take cultural aspects into account in its action.

(13) A common search for, and consistent application at European level of, technical measures to protect works and other subject-matter while permitting exceptions or limitations in the public interest for the purpose of education and teaching.

(15) The Diplomatic Conference held under the auspices of the World Intellectual Property Organisation (WIPO) in December 1996 led to the adoption of two new Treaties, the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty", dealing respectively with the protection of authors and the protection of performers and phonogram producers. Those Treaties update the international protection for copyright and related rights significantly, not least with regard to the so-called "digital agenda", and improve the means to fight piracy world-wide. The Community and a majority of Member States have already signed the Treaties and the process of making arrangements for the ratification of the Treaties by the Community and the Member States is under way. This Directive also serves to implement a number of the new international obligations.
[16] Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce") (4), which clarifies and harmonises various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.

[17] It is necessary, especially in the light of the requirements arising out of the digital environment, to ensure that collecting societies achieve a higher level of rationalisation and transparency with regard to compliance with competition rules.

[18] This Directive is without prejudice to the arrangements in the Member States concerning the management of rights such as extended collective licences.

[19] The moral rights of rightholders should be exercised according to the limitations of the Member States and the provisions of the Berne Convention on Literary and Artistic Works, of the WIPO Copyright Treaty and of the WIPO Performances and Phonograms Treaty. Such moral rights remain outside the scope of this Directive.

[20] This Directive is based on principles and rules already laid down in the Directives currently in force in this area, in particular Directives 91/250/EEC (5), 92/100/EEC (6), 93/83/EEC (7), 93/98/EEC (8) and 96/9/EC (9), and it develops those principles and rules and places them in the context of the information society. The provisions of this Directive should be without prejudice to the provisions of those Directives, unless otherwise provided in this Directive.

[21] This Directive should define the scope of the acts covered by the reproduction right with regard to the different beneficiaries. This should be done in conformity with the acquis communautaire. A broad definition of these acts is needed to ensure legal certainty within the internal market.

[22] The objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeit or pirated works.

[23] This Directive should harmonise further the author's right of communication to the public. This right should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts.

[24] The right to make available to the public subject-matter referred to in Article 3(2) should be understood as covering all acts of making available such subject-matter to members of the public not present at the place where the act of making available originates, and as not covering any other acts.

[25] The legal uncertainty regarding the nature and the level of protection of acts of on-demand transmission of copyright works and subject-matter protected by related rights over networks should be overcome by providing for harmonised protection at Community level. It should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterised by the fact that members of the public may access them from a place and at a time individually chosen by them.

[26] With regard to the making available in on-demand services by broadcasters of their radio or television productions incorporating music from commercial phonograms as an integral part thereof, collective licensing arrangements are to be encouraged in order to facilitate the clearance of the rights concerned.

[27] The mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive.

[28] Copyright protection under this Directive includes the exclusive right to retransmit a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts.

[29] The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original copies of works and the corresponding subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides.

[30] The rights referred to in this Directive may be transferred, assigned or subject to the granting of contractual licences, without prejudice to the relevant national legislation on copyright and related rights.

[31] A fair balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded. The existing exceptions and limitations to the rights as set out by the Member States have to be reassessed in the light of the new electronic environment. Existing differences in the exceptions and limitations to certain restricted acts have direct negative effects on the functioning of the internal market of copyright and related rights. Such differences could well become more pronounced in view of the further development of transborder exploitation of works and cross-border activities. In order to ensure the proper functioning of the internal market, such exceptions and limitations should be defined in a harmonious manner. The degree of their harmonisation should be based on their impact on the smooth functioning of the internal market.

[32] This Directive provides for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public. Some exceptions or limitations only apply to the reproduction right, where appropriate. This list takes due account of the different legal traditions in Member States, while, at the same time, aiming to ensure a functioning internal market. Member States should arrive at a coherent application of these exceptions and limitations, which will be assessed when reviewing implementing legislation in the future.

[33] The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own. To the extent that they meet these conditions, this exception should include acts...
which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use of information, so far as it is concerned, is any use of the information made in the context of on-line delivery of protected works or other subject-matter. When determining the form, detailed arrangements and possible level of such fair compensation, account should be taken of the particular circumstances of each case. When evaluating these circumstances, a valuable criterion would be the possible harm to the rightholders resulting from the act in question. In cases where rightholders have already received payment in some other form, for instance as part of a licence fee, no specific or separate payment may be due. The level of fair compensation should take full account of the degree of use of the technological protection measures referred to in this Directive. In certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise.

(36) The Member States may provide for fair compensation for rightholders also when applying the optional provisions on exceptions or limitations which do not require such compensation.

(37) Existing national schemes on reprography, where they exist, do not create major barriers to the internal market. Member States should be allowed to provide for an exception or limitation in respect of reprography.

(38) Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audio-visual material for private use, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. Although differences between those remuneration schemes affect the functioning of the internal market, those differences, with respect to analogue private reproduction, should not have a significant impact on the development of the information society. Digital private copying could potentially involve a greater increase in economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.

(39) When applying the exception or limitation on private copying, Member States should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available. Such exceptions or limitations should not inhibit the use of technological measures or their enforcement against circumvention.

(40) Member States may provide for an exception or limitation for the benefit of certain non-profit making establishments, such as publicly accessible libraries and equivalent institutions, as well as archives. However, this should be limited to certain special cases covered by the reproduction right. Such an exception or limitation should not cover uses made in the context of on-line delivery of protected works or other subject-matter. This Directive should be without prejudice to the Member States’ option to derogate from the exclusive public lending right in accordance with Article 5 of Directive 92/100/EEC. Therefore, specific contracts or licences should be promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve.

(41) When applying the exception or limitation in respect of ephemeral recordings made by broadcasting organisations it is understood that a broadcasting organisation may be considered lawful where it is authorised by the rightholder or not restricted by law.

(42) When applying the exception or limitation for non-commercial educational and scientific research purposes, including distance learning, the non-commercial nature of the activity in question should be determined by that activity as such. The organisational structure and the means of funding of the establishment concerned are not the decisive factors in this respect.

(43) It is in any case important for the Member States to adopt all necessary measures to facilitate access to works by persons suffering from a disability which constitutes an obstacle to the use of the works themselves, and to pay particular attention to accessible formats.

(44) When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the rightholder or which conflicts with the normal exploitation of his work or other subject-matter. The provision of such exceptions or limitations by Member States should, in particular, duly reflect the increased economic impact that such exceptions or limitations may have in the context of the new electronic environment. Therefore, the scope of certain exceptions or limitations may have to be even more limited when it comes to certain new uses of copyright works and other subject-matter.

(45) The exceptions and limitations referred to in Article 5(2), (3) and (4) should not, however, prevent the definition of contractual relations designed to ensure fair compensation for the rightholders insofar as permitted by national law.

(46) Recourse to mediation could help users and rightholders to settle disputes. The Commission, in cooperation with the Member States within the Contact Committee, should undertake a study to consider new legal ways of settling disputes concerning copyright and related rights.

(47) Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder innovation and have a greater economic impact, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

(48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases, without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a certain significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography.

(49) The legal protection of technological measures is without prejudice to the application of any national provisions which may prohibit the private possession of devices, products or components for the circumvention of technological measures.
Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological means used in connection with computer programs, which is exclusively addressed in that Directive. It should neither hinder nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determines exceptions to the exclusive rights applicable to computer programs.

The legal protection of technological measures applies without prejudice to public policy, as reflected in Article 5, or public security. Member States should promote voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided in national law in accordance with this Directive. In the absence of such voluntary measures or agreements within a reasonable period of time, Member States should take appropriate measures to ensure that rightholders provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological measure or by other means. However, in order to prevent abuse of such measures taken by rightholders, including agreements between rightholders and other parties concerned, as well as measures taken by Member States, do not prevent rightholders from using technological measures which are consistent with the exceptions or limitations on private copying in national law in accordance with Article 5(2)b, taking account of the condition of fair compensation under that provision and the possible differentiation between various conditions of use in accordance with Article 5(5), such as controlling the number of reproductions. In order to prevent abuse of such measures, any technological measures applied in their implementation should enjoy legal protection.

The protection of technological measures should ensure a secure environment for the provision of interactive on-demand services, in such a way that members of the public may access works or other subject-matter from a place and at a time individually chosen by them. Where such services are governed by contractual arrangements, the first and second subparagraphs of Article 6(4) should not apply. Non-interactive forms of online use should remain subject to those provisions.

Important progress has been made in the international standardisation of technical systems of identification of works and protected subject-matter in digital format. In an increasingly networked environment, differences between technological means could lead to an incompatibility of systems within the Community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems.

Technological development will facilitate the distribution of works, notably on networks, and this will entail the need for rightholders to identify better the work or other subject-matter, the author or any other rightholder, and to provide information about the terms and conditions of use of the work or other subject-matter in order to render easier the management of rights attached to them. Rightholders should be encouraged to use markings indicating, in addition to the information referred to above, inter alia their authorisation when putting works or other subject-matter on networks. There is, however, the danger that illegal activities might be carried out in order to remove or alter the electronic copyright-management information attached to it, or otherwise to distribute, import for distribution, broadcast, communicate to the public or make available to the public works or other protected subject-matter from which such information has been removed without authority. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against any of these activities.

Any such rights-management information systems referred to above may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means of their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even when the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

The protection provided under this Directive should be without prejudice to national or Community legal provisions in other areas, such as industrial property, data protection, conditional access, access to public documents, and the rule of media exploitation chronology, which may affect the protection of copyright or related rights.

In order to comply with the WIPO Performances and Phonograms Treaty, Directives 92/100/EEC and 93/98/EEC should be amended.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
OBJECTIVE AND SCOPE

Article 1
Scope
1. This Directive concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.
2. Except in the cases referred to in Article 11, this Directive shall leave intact and shall in no way affect existing Community provisions relating to:
   (a) the legal protection of computer programs;
   (b) rental right, lending right and certain rights related to copyright in the field of industrial property;
(c) copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission;
(d) the term of protection of copyright and certain related rights;
(e) the legal protection of databases.

CHAPTER II
RIGHTS AND EXCEPTIONS

Article 2
Reproduction right
Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:
(a) of authors, of their works;
(b) for performers, of fixations of their performances;
(c) for phonogram producers, of their phonograms;
(d) for the producers of the first fixations of films, in respect of the original and copies of their films;
(e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

Article 3
Right of communication to the public of works and right of making available to the public of other subject-matter
1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them:
(a) for performers, of fixations of their performances;
(b) for phonogram producers, of their phonograms;
(c) for the producers of the first fixations of films, of the original and copies of their films;
(d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.
2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
(a) for performers, of fixations of their performances;
(b) for phonogram producers, of their phonograms;
(c) for the producers of the first fixations of films, of the original and copies of their films;
(d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

Article 4
Distribution right
1. Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.
2. The distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.

Article 5
Exceptions and limitations
1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
(a) a transmission in a network between third parties by an intermediary, or
(b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.
2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:
(a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;
(b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;
(c) in respect of specific acts of reproduction made by publicly accessible libraries, educational institutions, museums, or by archives, which are not for direct or indirect economic or commercial advantage;
(d) in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of those recordings in official archives may, on the grounds of their exceptional documentary character, be permitted;
(e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.
3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:
(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author’s name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;
(b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;
(c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author’s name, is indicated, unless this turns out to be impossible;
(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author’s name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;
(e) use for the purposes of public security or to ensure the proper performance of administrative, parliamentary or judicial proceedings;
(f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informative purpose and provided that the source, including the author’s name, is indicated, except where this turns out to be impossible;
(g) use during religious celebrations or official celebrations organised by a public authority;
(h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;
(i) incidental inclusion of a work or other subject-matter in other material;
(j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;
(k) use for the purpose of caricature, parody or pastiche;
(l) use in connection with the demonstration or repair of equipment;
(m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;
(n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;
(o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

4. Where the Member States may provide for an exception or limitation to the right of reproduction pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.

5. The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.

CHAPTER III
PROTECTION OF TECHNOLOGICAL MEASURES AND RIGHTS-MANAGEMENT INFORMATION

Article 6
Obligations as to technological measures
1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
(a) are promoted, advertised or marketed for the purpose of circumvention of, or use other than to circumvent, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(c) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1. The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply mutatis mutandis.

Article 7
Obligations concerning rights-management information
1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:
(a) the removal or alteration of any electronic rights-management information;
(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.

2. For the purposes of this Directive, the expression "rights-management information" means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of a work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC.

CHAPTER IV
COMMON PROVISIONS

Article 8
Sanctions and remedies
1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.
2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

**Article 9**

**Continued application of other legal provisions**

This Directive shall be without prejudice to provisions concerning in particular patent rights, trade marks, design rights, utility models, topographies of semi-conductor products, type faces, conditional access, access to cable of broadcasting services, protection of national treasures, legal deposit requirements, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, the law of contract.

**Article 10**

**Application over time**

1. The provisions of this Directive shall apply in respect of all works and other subject-matter referred to in this Directive which are, on 22 December 2002, protected by the Member States’ legislation in the field of copyright and related rights, or which meet the criteria for protection under the provisions of this Directive or the provisions referred to in Article 1(2).

2. This Directive shall apply without prejudice to any acts concluded and rights acquired before 22 December 2002.

**Article 11**

**Technical adaptations**

1. Directive 92/100/EEC is hereby amended as follows:

   (a) Article 7 shall be deleted;

   (b) Article 10(3) shall be replaced by the following: “The limitations shall only be applied in certain special cases which do not conflict with a normal exploitation of the subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.”

2. Article 3(2) of Directive 93/98/EEC shall be replaced by the following: “The rights of producers of phonograms shall expire 50 years after the fixation is made. However, if the phonogram has been lawfully published within this period, the said rights shall expire 50 years from the date of the first lawful publication. If no lawful publication has taken place within the period mentioned in the first sentence, and if the phonogram has been lawfully communicated to the public within this period, the said rights shall expire 50 years from the date of the first lawful communication to the public.

   However, where through the expiry of the term of protection granted pursuant to this paragraph in its version before amendment by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society the rights of producers of phonograms are no longer protected on 22 December 2002, this paragraph shall not have the effect of protecting those rights anew.”

**Article 12**

**Final provisions**

1. Not later than 22 December 2004 and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, in which, inter alia, on the basis of specific information supplied by the Member States, it shall examine in particular the application of Articles 5, 6 and 8 in the light of the development of the digital market. In the case of Article 6, it shall examine in particular whether that Article confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures. Where necessary, in particular to ensure the functioning of the internal market pursuant to Article 14 of the Treaty, it shall submit proposals for amendments to this Directive.

2. Protection of rights related to copyright under this Directive shall leave intact and shall in no way affect the protection of copyright.

3. A contact committee is hereby established. It shall be composed of representatives of the competent authorities of the Member States. It shall be chaired by a representative of the Commission and shall meet either on the initiative of the chairman or at the request of the delegation of a Member State.

4. The tasks of the committee shall be as follows:

   (a) to examine the impact of this Directive on the functioning of the internal market, and to highlight any difficulties;

   (b) to organise consultations on all questions deriving from the application of this Directive;

   (c) to facilitate the exchange of information on relevant developments in legislation and case-law, as well as relevant economic, social, cultural and technological developments;

   (d) to act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures.

**Article 13**

**Implementation**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 22 December 2002. They shall forthwith inform the Commission thereof.

2. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

3. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field governed by this Directive.

**Article 14**

**Entry into force**

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

[...]
Relevant Case-Law on Directive 2001/29/EC

C-5/08 Infopaq International A/S v Danske Dagblades Forening

1. An act occurring during a data capture process, which consists of storing an extract of a protected work comprising 11 words and printing out that extract, is such as to come within the concept of reproduction in part within the meaning of Article 2 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, if the elements thus reproduced are the expression of the intellectual creation of their author; it is for the national court to make this determination.

2. The act of printing out an extract of 11 words, during a data capture process such as that at issue in the main proceedings, does not fulfil the condition of being transient in nature as required by Article 5(1) of Directive 2001/29 and, therefore, that process cannot be carried out without the consent of the relevant rightholders.

C-467/08 Padawan v SGAE

The concept of 'fair compensation', within the meaning of Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, is an autonomous concept of European Union law which must be interpreted uniformly in all the Member States that have introduced a private copying exception, irrespective of the power conferred on the Member States to determine, within the limits imposed by European Union law in particular by that directive, the form, detailed arrangements for financing and collection, and the level of that fair compensation.

Article 5(2)(b) of Directive 2001/29 must be interpreted as meaning that the 'fair balance' between the persons concerned means that fair compensation must be calculated on the basis of the criterion of the harm caused to authors of protected works by the introduction of the private copying exception. It is consistent with the requirements of that 'fair balance' to provide that persons who have digital reproduction equipment, devices and media and who on that basis, in law or in fact, make that equipment available to private users or provide them with copying services are the persons liable to finance the fair compensation, inasmuch as they are able to pass on to private users the actual burden of financing it.

Article 5(2)(b) of Directive 2001/29 must be interpreted as meaning that a link is necessary between the application of the levy intended to finance fair compensation with respect to digital reproduction equipment, devices and media and the deemed use of them for the purposes of private copying. Consequently, the indiscriminate application of the private copying levy, in particular with respect to digital reproduction equipment, devices and media not made available to private users and clearly reserved for uses other than private copying, is incompatible with Directive 2001/29.

C-462/09 Stichting de Thuiskopie v Opus Supplies Deutschland GmbH and Others

1. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, in particular Article 5(2)(b) and (5) thereof, must be interpreted as meaning that the final user who carries out, on a private basis, the reproduction of a protected work must, in principle, be regarded as the person responsible for paying the fair compensation provided for in Article 5(2)(b). However, it is open to the Member States to establish a private copying levy chargeable to the persons who make reproduction equipment, devices and media available to that final user, since they are able to pass on the amount of that levy in the price paid by the final user for that service.

2. Directive 2001/29, in particular Article 5(2)(b) and (5) thereof, must be interpreted as meaning that it is for the Member State which has introduced a system of private copying levies chargeable to the manufacturer or importer of media for reproduction of protected works, and on the territory of which the harm caused to authors by the use for private purposes of their work by purchasers who reside there occurs, to ensure that those authors actually receive the fair compensation intended to compensate them for that harm. In that regard, the mere fact that the commercial seller of reproduction equipment, devices and media is established in a Member State other than that in which the purchasers reside has no bearing on that obligation to achieve a certain result. It is for the national court, where it is impossible to ensure recovery of the fair compensation from the purchasers, to interpret national law in order to allow recovery of that compensation from the person responsible for payment who is acting on a commercial basis.


1. Article 6(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as not precluding its application solely because actions against several defendants for substantially identical copyright infringements are brought on national legal grounds which vary according to the Member States concerned. It is for the referring court to assess, in the light of all the elements of the case, whether there is a risk of irreconcilable judgments if those actions were determined separately.

2. Article 6 of Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights must be interpreted as meaning that a
portrait photograph can, under that provision, be protected by copyright if, which is it for the national court to determine in each case, such photograph is an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production of that photograph. Since it has been determined that the portrait photograph in question is a work, its protection is not inferior to that enjoyed by any other work, including other photographic works.

3. Article 5(3)(e) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, read in the light of Article 5(5) of that directive, must be interpreted as meaning that the media, such as newspaper publishers, may not use, of their own volition, a work protected by copyright by invoking an objective of public security. However, it is conceivable that a newspaper publisher might, in specific cases, contribute to the fulfilment of such an objective by publishing a photograph of a person for whom a search has been launched. It should be required that such initiative is taken, first, within the framework of a decision or action taken by the competent national authorities to ensure public security and, second, by agreement and in coordination with those authorities, in order to avoid the risk of interfering with the measures taken by them, without, however, a specific, current and express appeal, on the part of the security authorities, for publication of a photograph for the purposes of an investigation being necessary.

4. Article 5(3)(d) of Directive 2001/29, read in the light of Article 5(5) of that directive, must be interpreted as not precluding its application where a press report quoting a work as evidence of the facts, or for an unlimited period, as a preventative measure; which applies indiscriminately to all of those users; and certain related rights, must be interpreted as precluding a national court from setting aside national legislation contrary to that provision.

2. Article 3(1) of Directive 2001/29 must be interpreted as meaning that rights in the information society must be interpreted as meaning that rights to exploit the cinematographic work such as those at issue in the main proceedings (reproduction right, satellite broadcasting right and any other right of communication to the public through the making available to the public) vest by operation of law, directly and originally, in the principal director. Consequently, those provisions must be interpreted as precluding national legislation which allocates those exploitation rights by operation of law exclusively to the producer of the work in question.

3. European Union law must be interpreted as meaning that, in his capacity as author of a cinematographic work, the principal director thereof must be entitled, by operation of law, directly and originally, to the right to the fair compensation provided for in Article 5(2)(b) of Directive 2001/29 under the ‘private copying’ exception.

4. European Union law must be interpreted as not allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of rights to exploit the cinematographic work such as those at issue in the main proceedings (satellite broadcasting right, reproduction right and any other right of communication to the public through the making available to the public), provided that such a presumption is not an irrebuttable one precluding the principal director of that work from agreeing otherwise.

3. Articles 1 and 2 of Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, and Articles 2 and 3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society in conjunction with Articles 2 and 3 of Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property and with Article 2 of Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, must be interpreted as meaning that rights to exploit a cinematographic work such as those at issue in the main proceedings (reproduction right, satellite broadcasting right and any other right of communication to the public through the making available to the public) vest by operation of law, directly and originally, in the principal director. Consequently, those provisions must be interpreted as precluding national legislation which allocates those exploitation rights by operation of law exclusively to the producer of the work in question.

3. European Union law must be interpreted as meaning that, in his capacity as author of a cinematographic work, the principal director thereof must be entitled, by operation of law, directly and originally, to the right to the fair compensation provided for in Article 5(2)(b) of Directive 2001/29 under the ‘private copying’ exception.

4. European Union law must be interpreted as not allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of the right to fair compensation vesting in the principal director of that work, whether that presumption is couched in irrebuttable terms or may be departed from.

C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) v Netlog NV

Directives:
- 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);
- 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; and
- 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering:
- information which is stored on its servers by its service users;
- which applies indiscriminately to all of those users;
- as a preventative measure;
- exclusively at its expense; and
- for an unlimited period,
which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright.

C-277/10 Martin Luksan v Petrus van der Let

1. Articles 1 and 2 of Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, and Articles 2 and 3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society in conjunction with Articles 2 and 3 of Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property and with Article 2 of Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, must be interpreted as meaning that rights to exploit a cinematographic work such as those at issue in the main proceedings (reproduction right, satellite broadcasting right and any other right of communication to the public through the making available to the public) vest by operation of law, directly and originally, in the principal director. Consequently, those provisions must be interpreted as precluding national legislation which allocates those exploitation rights by operation of law exclusively to the producer of the work in question.

2. European Union law must be interpreted as allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of rights to exploit the cinematographic work such as those at issue in the main proceedings (satellite broadcasting right, reproduction right and any other right of communication to the public through the making available to the public), provided that such a presumption is not an irrebuttable one precluding the principal director of that work from agreeing otherwise.

3. European Union law must be interpreted as meaning that, in his capacity as author of a cinematographic work, the principal director thereof must be entitled, by operation of law, directly and originally, to the right to the fair compensation provided for in Article 5(2)(b) of Directive 2001/29 under the ‘private copying’ exception.

4. European Union law must be interpreted as not allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of the right to fair compensation vesting in the principal director of that work, whether that presumption is couched in irrebuttable terms or may be departed from.

C-351/12 OSA – Ochranný svaz autorský pro práva k dílům hudebním o.s. v Léčebné lázně Mariánské Lázně a.s.

1. Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as precluding national legislation which excludes the right of authors to authorise or prohibit the communication of their works, by a spa establishment which is a business, through the intentional distribution of a signal by means of television or radio sets in the bedrooms of the establishment’s patients. Article 5(2)(e), (3)(b) and (5) of that directive is not such as to affect that interpretation.

2. Article 3(1) of Directive 2001/29 must be interpreted as meaning that it cannot be relied on by a copyright collecting society in a dispute between individuals for the purpose of setting aside national legislation contrary to that provision. However, the national court hearing such a case is required to interpret that legislation, so far as possible, in the light of the
worrying and purpose of the directive in order to achieve an outcome consistent with the objective pursued by the directive.

3. Article 16 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, and Articles 56 TFEU and 102 TFEU must be interpreted as not precluding national legislation, such as that at issue in the main proceedings, which reserves the exercise of collective management of copyright in respect of certain protected works in the territory of the Member State concerned to a single copyright collecting society and thereby prevents users of such works, such as the spa establishment in the main proceedings, from benefiting from the services provided by another collecting society established in another Member State. However, Article 102 TFEU must be interpreted as meaning that the imposition by that copyright collecting society of fees for its services which are appreciably higher than those charged in other Member States (a comparison of the fee levels having been made on a consistent basis) or the imposition of a price which is excessive in relation to the economic value of the service provided are indicative of an abuse of a dominant position.

C-435/12 ACI Adam BV and Others v Stichting de Thuiskopie, Stichting Onderhandelingen Thuiskopie vergoeding,

1. EU law, in particular Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, read in conjunction with paragraph 5 of that article, must be interpreted as precluding national legislation, such as that at issue in the main proceedings, which does not distinguish the situation in which the source from which a reproduction for private use is made is lawful from that in which that source is unlawful.

2. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as not applying to proceedings, such as those in the main proceedings, in which those liable for payment of the fair compensation bring an action before the referring court for a ruling against the body responsible for collecting that remuneration and distributing it to copyright holders, which defends that action.

C-360/13 Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and Others

Article 5 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the copies on the user's computer screen and the copies in the internet 'cache' of that computer's hard disk, made by an end-user in the course of viewing a website, satisfy the conditions that those copies must be temporary, that they must be transient or incidental in nature and that they must constitute an integral and essential part of a technological process, as well as the conditions laid down in Article 5(5) of that directive, and that they may therefore be made without the authorisation of the copyright holders.

C-463/12 Copydan Båndkopi proti Nokia Danmark A/S.

1. Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society does not preclude national legislation which provides that fair compensation is to be paid, in accordance with the exception to the reproduction right for copies made for private use, in respect of multifunctional media such as mobile telephone memory cards, irrespective of whether the main function of such media is to make such copies, provided that one of the functions of the media, be it merely an ancillary function, enables the operator to use them for that purpose. However, the question whether the function is a main or an ancillary one and the relative importance of the medium's capacity to make copies are liable to affect the amount of fair compensation payable. In so far as the prejudice to the rightholder may be regarded as minimal, the making available of such a function need not give rise to an obligation to pay fair compensation.

2. Article 5(2)(b) of Directive 2001/29 does not preclude national legislation which makes the supply of media that may be used for copying for private use, such as mobile telephone memory cards, subject to the levy intended to finance fair compensation payable in accordance with the exception to the reproduction right for copies for private use, but does not make the supply of components whose main purpose is to store copies for private use, such as the internal memories of MP3 players, subject to that levy, provided that those different categories of media and components are not comparable or the different treatment they receive is justified, which is a matter for the national court to determine.

3. Article 5(2)(b) of Directive 2001/29 must be interpreted as not precluding national legislation which requires payment of the levy intended to finance fair compensation, in accordance with the exception to the reproduction right for copies for private use, by producers and importers who sell mobile telephone memory cards to business customers and are aware that those cards will be sold on by those customers but do not know whether the final purchasers of the cards will be individuals or business customers, on condition that:

- the introduction of such a system is justified by practical difficulties;
- the persons responsible for payment are exempt from the levy if they can establish that they have supplied the mobile telephone memory cards to persons other than natural persons for purposes clearly unrelated to copying for private use, it being understood that the exemption cannot be restricted to the supply of business customers registered with the organisation responsible for administering the levy;
- the system provides for a right to reimbursement of that levy which is effective and does not make it excessively difficult to repay the levy and only the final purchaser of such a memory card may obtain reimbursement by submitting an appropriate application to that organisation.

4. Article 5(2)(b) of Directive 2001/29, read in the light of recital 35 in the preamble to that directive, must be interpreted as permitting the Member States to provide, in certain cases covered by the exception to the reproduction right for copies for private use, for an exemption from the requirement under that exception to pay fair compensation, provided that the prejudice caused to rightholders in such cases is minimal. It is within the discretion of the Member States to set the threshold for such prejudice, it being understood that that threshold must, inter alia, be applied in a manner consistent with the principle of equal treatment.

5. Directive 2001/29 is to be interpreted as meaning that, where a Member State has decided, pursuant to Article 5(2) of that directive, to exclude, from the material scope of that provision, any right for rightholders to authorise reproduction of their works for private use, for an exception from the requirement under that exception to pay fair compensation, the prejudice caused to rightholders in such cases is minimal. It is within the discretion of the Member States to set the threshold for such prejudice, it being understood that that threshold must, inter alia, be applied in a manner consistent with the principle of equal treatment.

6. The implementation of technological measures under Article 6 of Directive 2001/29 for devices used to reproduce protected works, such as DVDs, CDs, MP3 players and computers, can have no effect on the requirement to pay fair compensation in accordance with the exception to the
reproduction right in respect of reproductions made for private use by means of such devices. However, the implementation of such measures may have an effect on the actual level of such compensation.

7. Directive 2001/29 precludes national legislation which provides for fair compensation in accordance with the exception to the reproduction right, in respect of reproductions made using unlawful sources, namely from protected works which are made available to the public without the rightholder’s consent.

8. Directive 2001/29 does not preclude national legislation which provides for fair compensation, in accordance with the exception to the reproduction right, in respect of reproductions of protected works made by a natural person by or with the aid of a device which belongs to a third party.

C-466/12 Nils Svensson and Others v Retriever Sverige AB

1. Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, as must be interpreted as meaning that the provision on a website of clickable links to works freely available on another website does not constitute an ‘act of communication to the public’, as referred to in that provision.

2. Article 3(1) of Directive 2001/29 must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.

C-117/13 Technische Universität Darmstadt v Eugen Ulmer KG*

1. The concept of ‘purchase or licensing terms’ provided for in Article 5(3)(n) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be understood as requiring that the rightholder and an establishment, such as a publicly accessible library, referred to in that provision must have concluded a licensing agreement in respect of the works in question that sets out the conditions in which that establishment may use that work.

2. Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

3. Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that directive provided that, in each individual case, the conditions laid down by those provisions are met.

* For further reference see p. 110

C-201/13 Johan Deckmyn, Vrijheidsfonds VZW v Helena Vandersteen and others

1. Article 5(3)(k) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, must be interpreted as meaning that the concept of ‘parody’ appearing in that provision is an autonomous concept of EU law.

2. Article 5(3)(k) of Directive 2001/29 must be interpreted as meaning that the essential characteristics of parody, are, first, to evoke an existing work, while being noticeably different from it, and secondly, to constitute an expression of humour or mockery. The concept of ‘parody’, within the meaning of that provision, is not subject to the conditions that the parody should display an original character of its own, other than that of displaying noticeable differences with respect to the original parodied work; that it could reasonably be attributed to a person other than the author of the original work itself; that it should relate to the original work itself or mention the source of the parodied work.

However, the application, in a particular case, of the exception for parody, within the meaning of Article 5(3)(k) of Directive 2001/29, must strike a fair balance between, on the one hand, the interests and rights of persons referred to in Articles 2 and 3 of that directive, and, on the other, the freedom of expression of the user of a protected work who is relying on the exception for parody, within the meaning of Article 5(3)(k).

It is for the national court to determine, in the light of all the circumstances of the case in the main proceedings, whether the application of the exception for parody, within the meaning of Article 5(3)(k) of Directive 2001/29, on the assumption that the drawing at issue fulfils the essential requirements of parody, preserves that fair balance.

C-419/13 Art & Allposters International BV v Stichting Pictoright

Article 4(2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the rule of exhaustion of the distribution right set out in Article 4(2) of Directive 2001/29 does not apply in a situation where a reproduction of a protected work, after having been marketed in the European Union with the copyright holder’s consent, has undergone an alteration of its medium, such as the transfer of that reproduction from a paper poster onto a canvas, and is placed on the market again in its new form.

Directive 2009/24/EC on the legal protection of computer programs

of 23 April 2009
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community and in particular Article 95 thereof,

Having regard to the proposal from the Commission,
Having regard to the opinion of the European Economic and Social Committee [1],
Acting in accordance with the procedure laid down in Article
251 of the Treaty [2],
Whereas:
1991 on the legal protection of computer programs [3] has
been amended [4]. In the interests of clarity and rationality
the said Directive should be codified.
(2) The development of computer programs requires the
investment of considerable human, technical and financial
resources while computer programs can be copied at a
fraction of the cost needed to develop them independently.
(3) Computer programs are playing an increasingly important
role in a broad range of industries and computer program
technology can accordingly be considered as being of
fundamental importance for the Community's industrial
development.
(4) Certain differences in the legal protection of computer
programs offered by the laws of the Member States have direct
and negative effects on the functioning of the internal market
as regards computer programs.
(5) Existing differences having such effects need to be
removed and new ones prevented from arising, while
differences not adversely affecting the functioning of the
internal market to a substantial degree need not be removed
or prevented from arising.
(6) The Community's legal framework on the protection of
computer programs can accordingly in the first instance be
limited to establishing that Member States should accord
protection to computer programs under copyright law as
literary works and, further, to establishing who and what
should be protected, the exclusive rights on which protected
persons should be able to rely in order to authorise or prohibit
certain acts and for how long the protection should apply.
(7) For the purpose of this Directive, the term "computer
program" shall include programs in any form, including those
which are incorporated into hardware. This term also includes
preparatory work leading to the development of a
computer program provided that the nature of the
preparatory work is such that a computer program can result
from it at a later stage.
(8) In respect of the criteria to be applied in determining
whether or not a computer program is an original work, no
tests as to the qualitative or aesthetic merits of the program
should be applied.
(9) The Community is fully committed to the promotion of
international standardisation.
(10) The function of a computer program is to communicate
and work together with other components of a computer
system and with users and, where appropriate, with other
programs. It has therefore to be compatible with fair practice
and must therefore be defined as the
ability to exchange information and mutually to use the
information which has been exchanged.
(11) For the avoidance of doubt, it has to be made clear that
only the expression of a computer program is protected and
that ideas and principles which underlie any element of a
program, including those which underlie its interfaces, are not
protected by copyright under this Directive. In accordance
with this principle of copyright, to the extent that logic,
algorithms and programming languages comprise ideas and
principles, those ideas and principles are not protected under
this Directive. In accordance with the legislation and case-law
of the Member States and the international copyright
conventions, the expression of those ideas and principles is to
be protected by copyright.
(12) For the purposes of this Directive, the term "rental"
means the making available for use, for a limited period of
time and for profit-making purposes, of a computer program
or a copy thereof. This term does not include public lending,
which, accordingly, remains outside the scope of this Directive.
(13) The exclusive rights of the author to prevent the
unauthorised reproduction of his work should be subject to a
limited exception in the case of a computer program to allow
the reproduction technically necessary for the use of that
program by the lawful acquirer. This means that the acts of
loaning and running necessary for the use of a copy of a
program which has been lawfully acquired, and the act of
correction of its errors, may not be prohibited by contract.
In the absence of specific contractual provisions, including when
a copy of the program has been sold, any other act necessary
for the use of the copy of a program may be performed in
accordance with its intended purpose by a lawful acquirer of
that copy.
(14) A person having a right to use a computer program
should not be prevented from performing acts necessary to
observe, study or test the functioning of the program,
provided that those acts do not infringe the copyright in
the program.
(15) The unauthorised reproduction, translation, adaptation
or transformation of the form of the code in which a copy of a
computer program has been made available constitutes an
infringement of the exclusive rights of the author.
Nevertheless, circumstances may exist when such a
reproduction of the code and translation of its form are
indispensable to obtain the necessary information to achieve
the interoperability of an independently created program with
other programs. It has therefore to be considered that, in these
limited circumstances only, performance of the acts of
reproduction and translation by or on behalf of a person
having a right to use a copy of the program is legitimate and
compatible with fair practice and must therefore be
done not to require the authorisation of the rightholder. An
objective of this exception is to make it possible to connect all
components of a computer system, including those of different
manufacturers, so that they can work together. Such an
exception to the author's exclusive rights may not be used in a
way which prejudices the legitimate interests of the
rightholder or which conflicts with a normal exploitation
of the program.
(16) Protection of computer programs under copyright laws
should be without prejudice to the application, in appropriate
cases, of other forms of protection. However, any contractual
provisions contrary to the provisions of this Directive laid
down in respect of decompilation or to the exceptions
provided for by this Directive with regard to the making of
a back-up copy or to the examination, study or testing of
the functioning of a program should be null and void.
(17) The provisions of this Directive are without prejudice to
the application of the competition rules under Articles 81 and
82 of the Treaty if a dominant supplier refuses to make
information available which is necessary for interoperability
as defined in this Directive.
(18) The provisions of this Directive should be without
prejudice to specific requirements of Community law already
enacted in respect of the publication of interfaces in the
telecommunications sector or Council Decisions relating to
standardisation in the field of information technology and
telecommunication.
(19) This Directive does not affect derogations provided for
under national legislation in accordance with the Berne
Convention on points not covered by this Directive.
(20) This Directive should be without prejudice to the
obligations of the Member States relating to the time-limits for
transposition into national law of the Directives set out in
Annex I, Part B,
HAVE ADOPTED THIS DIRECTIVE:

Article 1
Object of protection
1. In accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works. For the purposes of this Directive, the term "computer programs" shall include their preparatory design material.

2. Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.

3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.

4. The provisions of this Directive shall apply also to programs created before 1 January 1993, without prejudice to any acts concluded and rights acquired before that date.

Article 2
Authorship of computer programs

1. The author of a computer program shall be the natural person or group of natural persons who has created the program or, where the legislation of the Member State permits, the legal person designated as the rightholder by that legislation.

Where collective works are recognised by the legislation of a Member State, the person considered by the legislation of the Member State to have created the work shall be deemed to be its author.

2. In respect of a computer program created by a group of natural persons jointly, the exclusive rights shall be owned jointly.

3. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

Article 3
Beneficiaries of protection

Protection shall be granted to all natural or legal persons eligible under national copyright legislation as applied to literary works.

Article 4
Restricted acts

1. Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2 shall include the right to do or to authorise:

(a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightholder;

(b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;

(c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof.

2. The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

Article 5
Exceptions to the restricted acts

1. In the absence of specific contractual provisions, the acts referred to in points (a) and (b) of Article 4(1) shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract in so far as it is necessary for that use.

3. The person having a right to use a copy of a computer program shall be entitled, without the authorisation of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Article 6
Decompiation

1. The authorisation of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

(c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or

(c) to be used for the development, production, or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program.

Article 7
Special measures of protection

1. Without prejudice to the provisions of Articles 4, 5 and 6, Member States shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the following acts:

(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

(b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

(c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the Member State concerned.

3. Member States may provide for the seizure of any means referred to in point (c) of paragraph 1.

Article 8
Continued application of other legal provisions

The provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent
This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

[...]  

### Relevant Case-Law on Directive 2009/24/EC

**C-393/09 Bezpečnostní softwarová asociace – Svaž softwarové ochrany v Ministerstvo Kultury**

1. A graphic user interface is not a form of expression of a computer program within the meaning of Article 1(2) of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs and cannot be protected by copyright as a computer program under that directive. Nevertheless, such an interface can be protected by copyright as a work by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society if that interface is its author’s own intellectual creation.

2. Television broadcasting of a graphic user interface does not constitute communication to the public of a work protected by copyright within the meaning of Article 3(1) of Directive 2001/29.

**C-406/10 SAS Institute Inc. v World Programming Ltd**

1. Article 1(2) of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs must be interpreted as meaning that neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program and, as such, are not protected by copyright in computer programs for the purposes of that directive.

2. Article 5(3) of Directive 91/250 must be interpreted as meaning that a person who has obtained a copy of a computer program under a licence is entitled, without the authorisation of the owner of the copyright, to observe, study or test the functioning of that program so as to determine the ideas and principles which underlie any element of the program, in the case where that person carries out acts covered by that licence and acts of loading and running necessary for the use of the computer program, and on condition that that person does not infringe the exclusive rights of the owner of the copyright in that program.

3. Article 2(a) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the reproduction, in a computer program or a user manual for that program, of certain elements described in the user manual for another computer program protected by copyright is capable of constituting an infringement of the copyright in the latter manual if - this being a matter for the national court to ascertain - that reproduction constitutes the expression of the intellectual creation of the author of the user manual for the computer program protected by copyright.

**C-128/11 UsedSoft GmbH v Oracle International Corp.**

1. Article 4(2) of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs must be interpreted as meaning that the right of distribution of a copy of a computer program is exhausted if the copyright holder who has authorised, even free of charge, the downloading of that copy from the internet onto a data carrier has also conferred, in return for payment of a fee intended to enable him to obtain a remuneration corresponding to the economic value of the copy of the work of which he is the proprietor, a right to use that copy for an unlimited period.

2. Articles 4(2) and 5(1) of Directive 2009/24 must be interpreted as meaning that, in the event of the resale of a user licence entailing the resale of a copy of a computer program downloaded from the copyright holder’s website, that licence having originally been granted by that rightholder to the first acquirer for an unlimited period in return for payment of a fee intended to enable the rightholder to obtain a remuneration corresponding to the economic value of that copy of his work, the second acquirer of the licence, as well as any subsequent acquirer of it, will be able to rely on the exhaustion of the distribution right under Article 4(2) of that directive, and hence be regarded as lawful acquirers of a copy of a computer program within the meaning of Article 5(1) of that directive and benefit from the right of reproduction provided for in that provision.


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 57 (2), 66 and 100a thereof,
 Having regard to the proposal from the Commission (1),
 Having regard to the opinion of the Economic and Social Committee (2),
 Acting in accordance with the procedure laid down in Article 189b of the Treaty (3),
 (1) Whereas databases are at present not sufficiently protected in all Member States by existing legislation; whereas such protection, where it exists, has different attributes; (2) Whereas such differences in the legal protection of databases offered by the legislation of the Member States have direct negative effects on the functioning of the internal market as regards databases and in particular on the freedom of natural and legal persons to provide on-line database goods and services on the basis of harmonized legal arrangements throughout the Community; whereas such differences could well become more pronounced as Member States introduce new legislation in this field, which is now taking on an increasingly international dimension; (3) Whereas existing differences distorting the functioning of the internal market need to be removed and new ones prevented from arising, while differences not adversely affecting the functioning of the internal market or the development of an information market within the Community need not be removed or prevented from arising; (4) Whereas copyright protection for databases exists in varying forms in the Member States according to legislation or case-law, and whereas, if differences in legislation in the scope and conditions of protection remain between the Member States, such unharmonized intellectual property rights can have the effect of preventing the free movement of goods or services within the Community; (5) Whereas copyright remains an appropriate form of exclusive right for authors who have created databases; (6) Whereas, nevertheless, in the absence of a harmonized system of unfair-competition legislation or of case-law, other measures are required in addition to prevent the unauthorized extraction and/or re-utilization of the contents of a database; (7) Whereas the making of databases requires the investment of considerable human, technical and financial resources while such databases can be copied or accessed at a fraction of the cost needed to design them independently; (8) Whereas the unauthorized extraction and/or re-utilization of the contents of a database constitute acts which can have serious economic and technical consequences; (9) Whereas databases are a vital tool in the development of an information market within the Community; whereas this tool also provides a basis in many other fields; (10) Whereas the exponential growth, in the Community and worldwide, in the amount of information generated and processed annually in all sectors of commerce and industry calls for investment in all the Member States in advanced information processing systems; (11) Whereas there is at present a very great imbalance in the level of investment in the database sector both as between the Member States and between the Community and the world’s largest database-producing third countries; (12) Whereas such an investment in modern information storage and processing systems will not take place within the Community unless a stable and uniform legal protection regime is introduced for the protection of the rights of makers of databases; (13) Whereas this Directive protects collections, sometimes called "compilations", of works, data or other materials which are arranged, stored and accessed by means which include electronic, electromagnetic or electro-optical processes or analogous processes; (14) Whereas protection under this Directive should be extended to cover non-electronic databases; (15) Whereas the criteria used to determine whether a database should be protected by copyright should be defined to the fact that the selection or the arrangement of the contents of the database is the author’s own intellectual creation; whereas such protection should cover the structure of the database; (16) Whereas no criterion other than originality in the sense of the author’s intellectual creation should be applied to determine the eligibility of the database for copyright protection, and in particular no aesthetic or qualitative criteria should be applied; (17) Whereas the term ‘database’ should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data; whereas it should cover collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed; whereas this means that a recording or an audiovisual, literary or musical work as such does not fall within the scope of this Directive; (18) Whereas this Directive is without prejudice to the freedom of authors to decide whether, or in what manner, they will allow their works to be included in a database, in particular whether or not the authorization given is exclusive; whereas the protection of databases by the sui generis right is without prejudice to existing rights over their contents, and whereas in particular where an author or the holder of a related right permits some of his works or subject matter to be included in a database pursuant to a non-exclusive agreement, a third party may make use of those works or subject matter without the consent of the holder of the related right or the maker of the database being invoked to prevent him doing so, on condition that those works or subject matter are neither extracted from the database nor re-utilized on the basis thereof; (19) Whereas, as a rule, the compilation of several recordings of musical performances on a CD does not come within the scope of this Directive, both because, as a compilation, it does not meet the conditions for copyright protection and because it does not represent a substantial enough investment to be eligible under the sui generis right; (20) Whereas protection under this Directive may also apply to the materials necessary for the operation or consultation of certain databases such as thesaurus and indexation systems; (21) Whereas the protection provided for in this Directive relates to databases in which works, data or other materials which have been arranged systematically or methodically; whereas it is not necessary for those materials to have been physically stored in an organized manner; (22) Whereas electronic databases within the meaning of this Directive may also include devices such as CD-ROM and CD-i; (23) Whereas the term ‘database’ should be extended to computer programs used in the making or operation of a database, which are protected by Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (4); (24) Whereas the rental and lending of databases in the field of copyright and related rights are governed exclusively by Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of industrial property (5); (25) Whereas the term of copyright is already governed by Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights (6); (26) Whereas works protected by copyright and subject matter protected by related rights, which are incorporated into a database, remain nevertheless protected by the respective exclusive rights and may not be incorporated into, or extracted from, the database without the permission of the rightholder or his successors in title; (27) Whereas copyright in such works and related rights in subject matter thus incorporated into a database are in no way affected by the existence of a separate right in the selection or arrangement of these works and subject matter in a database;
Whereas the moral rights of the natural person who created the database belong to the author and should be exercised according to the legislation of the Member States and the provisions of the Berne Convention for the Protection of Literary and Artistic Works; whereas such moral rights remain outside the scope of this Directive;

Whereas the arrangements applicable to databases created by employees are left to the discretion of the Member States; whereas, therefore nothing in this Directive prevents Member States from stipulating in their legislation that where a database is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the database so created, unless otherwise provided by contract;

Whereas the author's exclusive rights should include the right to determine the way in which the work is exploited and by whom, and in particular to control the distribution of his work to unauthorized persons;

Whereas the copyright protection of databases includes making databases available by means other than the distribution of copies;

Whereas Member States are required to ensure that their national provisions are at least materially equivalent in the case of such acts subject to restrictions as are provided for by this Directive;

Whereas the question of exhaustion of the right of distribution does not arise in the case of on-line databases, which come within the field of provision of services; whereas this also applies with regard to a material copy of such a database made by the user of such a service with the consent of the rightholder; whereas, unlike CD-ROM or CD-i, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which will have to be subject to authorization where the copyright so provides;

Whereas, nevertheless, once the rightholder has chosen to make available a copy of the database to a user, whether by an on-line service or by other means of distribution, that lawful user must be able to access and use the database for the purposes and in the way set out in the agreement with the rightholder, even if such access and use necessitate performance of otherwise restricted acts;

Whereas a list should be drawn up of exceptions to restricted acts taking into account the fact that copyright as covered by this Directive applies only to the selection or arrangements of the contents of a database; whereas Member States should be given the option of providing for such exceptions in certain cases; whereas, however, this option should be exercised in accordance with the Berne Convention and to the extent that the exceptions relate to the structure of the database; whereas a distinction should be drawn between exceptions for private use and exceptions for reproduction for private purposes, which concerns provisions under national legislation of some Member States on levies on blank media or recording equipment;

Whereas the term 'scientific research' within the meaning of this Directive covers both the natural sciences and the human sciences;

Whereas Article 10 (1) of the Berne Convention is not affected by this Directive;

Whereas the increasing use of digital recording technology exposes the database maker to the risk that the contents of his database may be copied and rearranged electronically, without his authorization, to produce a database of identical content which, however, does not infringe any copyright in the arrangement of his database;

Whereas, in addition to aiming to protect the copyright in the original selection or arrangement of the contents of a database, this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor;

Whereas the object of this sui generis right is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right; whereas such investment may consist in the deployment of financial resources and/or the expending of time, effort and energy;

Whereas the objective of the sui generis right is to give the maker of a database the option of preventing the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database; whereas the maker of a database is the person who takes the initiative and the risk of investing; whereas this excludes subcontractors in particular from the definition of maker;

Whereas the special right to prevent unauthorized extraction and/or re-utilization relates to acts by the user which go beyond his legitimate rights and thereby harm the investment; whereas the right to prohibit extraction and/or re-utilization of all or a substantial part of the contents relates not only to the manufacture of a parasitical competing product but also to any user who, through his acts, causes significant detriment, evaluated qualitatively or quantitatively, to the investment;

Whereas, in the case of on-line transmission, the right to prohibit re-utilization is not exhausted either as regards the database or as regards a material copy of the database or of part thereof made by the addressee of the transmission with the consent of the rightholder;

Whereas, when on-screen display of the contents of a database necessitates the permanent or temporary transfer of all or a substantial part of such contents to another medium, that act should be subject to authorization by the rightholder;

Whereas the objective of this Directive, which is to afford an extension of copyright protection to mere facts or data;

Whereas the existence of a right to prevent the unauthorized extraction and/or re-utilization of the whole or a substantial part of works, data or materials from a database should not give rise to the creation of a new right in the works, data or materials themselves;

Whereas, in the interests of competition between suppliers of information products and services, protection by the sui generis right must not be afforded in such a way as to facilitate abuses of a dominant position, in particular as regards the creation and distribution of new products and services which have an intellectual, documentary, technical, economic or commercial added value; whereas, therefore, the provisions of this Directive are without prejudice to the application of Community or national competition rules;

Whereas the objective of this Directive, which is to afford an appropriate and uniform level of protection of databases as a means to secure the remuneration of the maker of the database, is different from the aim of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (7), which is to guarantee free circulation of personal data on the basis of harmonized rules designed to protect fundamental rights, notably the right to privacy which is recognized in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas the provisions of this Directive are without prejudice to data protection legislation;

Whereas, notwithstanding the right to prevent extraction and/or re-utilization of all or a substantial part of a database, it should be laid down that the maker of a database or rightholder may not prevent a lawful user of the database from extracting and re-utilizing insubstantial parts; whereas, however, that user may not unreasonably prejudice either the legitimate interests of the holder of the sui generis right or the holder of copyright or a related right in respect of the works or subject matter contained in the database;
(50) Whereas the Member States should be given the option of providing for exceptions to the right to prevent the unauthorized extraction and/or re-utilization of a substantial part of the contents of a database in the case of extraction for private purposes, for the purposes of illustration for teaching or scientific research, or where extraction and/or re-utilization are/is carried out in the interests of public security or for the purposes of an administrative or judicial procedure; whereas such operations must not prejudice the exclusive rights of the maker to exploit the database and their purpose must not be commercial;
(51) Whereas the Member States, where they avail themselves of the option to permit a lawful user of a database to extract a substantial part of the contents for the purposes of illustration for teaching or scientific research, may limit that permission to certain categories of teaching or scientific research institutions;
(52) Whereas those Member States which have specific rules providing for a right comparable to the sui generis right provided for in this Directive should be permitted to retain, as far as the new right is concerned, the exceptions traditionally specified by such rules;
(53) Whereas the burden of proof regarding the date of completion of the making of a database lies with the maker of the database;
(54) Whereas the burden of proof that the criteria exist for concluding that a substantial modification of the contents of a database is to be regarded as a substantial new investment lies with the maker of the database resulting from such investment;
(55) Whereas a substantial new investment involving a new term of protection may include a substantial verification of the contents of the database;
(56) Whereas the right to prevent unauthorized extraction and/or re-utilization in respect of a database should apply to databases whose makers are nationals or habitual residents of third countries or to those produced by legal persons not established in a Member State, within the meaning of the Treaty, only if such third countries offer comparable protection to databases produced by nationals of a Member State or persons who have their habitual residence in the territory of the Community;
(57) Whereas, in addition to remedies provided under the legislation of the Member States for infringements of copyright or other rights, Member States should provide for appropriate remedies against unauthorized extraction and/or re-utilization of the contents of a database;
(58) Whereas, in addition to the protection given under this Directive to the structure of the database by copyright, and to its contents against unauthorized extraction and/or re-utilization under the sui generis right, other legal provisions in the Member States relevant to the supply of database goods and services continue to apply;
(59) Whereas this Directive is without prejudice to the application to databases composed of audiovisual works of any rules recognized by a Member State’s legislation concerning the broadcasting of audiovisual programmes;
(60) Whereas some Member States currently protect under copyright arrangements databases which do not meet the criteria for eligibility for copyright protection laid down in this Directive; whereas, even if the databases concerned are eligible for protection under the right laid down in this Directive to prevent unauthorized extraction and/or re-utilization of their contents, the term of protection under that right is considerably shorter than that which they enjoy under the national arrangements currently in force; whereas harmonization of the criteria for determining whether a database is to be protected by copyright may not have the effect of reducing the term of protection currently enjoyed by the rightholders concerned; whereas a derogation should be laid down to that effect; whereas the effects of such derogation must be confined to the territories of the Member States concerned.

H ave adopted this Directive:

CHAPTER I
SCOPE
Article 1
Scope

1. This Directive concerns the legal protection of databases in any form.
2. For the purposes of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
3. Protection under this Directive shall not apply to computer programs used in the making or operation of databases accessible by electronic means.

Article 2
Limitations on the scope
This Directive shall apply without prejudice to Community provisions relating to:
(a) the legal protection of computer programs;
(b) rental right, lending right and certain rights related to copyright in the field of intellectual property;
(c) the term of protection of copyright and certain related rights.

CHAPTER II
COPYRIGHT
Article 3
Object of protection
1. In accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author’s own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection.
2. The copyright protection of databases provided for by this Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves.

Article 4
Database authorship
1. The author of a database shall be the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the right holder by that legislation.
2. Where collective works are recognized by the legislation of a Member State, the economic rights shall be owned by the person holding the copyright.
3. In respect of a database created by a group of natural persons jointly, the exclusive rights shall be owned jointly.

Article 5
Restricted acts
In respect of the expression of the database which is protectable by copyright, the author of a database shall have the exclusive right to carry out or to authorize:
(a) temporary or permanent reproduction by any means and in any form, in whole or in part;
(b) translation, adaptation, arrangement and any other alteration;
(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;
(d) any communication, display or performance to the public;
(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).

Article 6
Exceptions to restricted acts
1. The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the
databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database. Where the lawful user is authorized to use only part of the database, this provision shall apply only to that part.

2. Member States shall have the option of providing for limitations on the rights set out in Article 5 in the following cases:

(a) in the case of reproduction for private purposes of a non-electronic database;

(b) where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;

(c) where there is use for the purposes of public security of for the purposes of an administrative or judicial procedure;

(d) where other exceptions to copyright which are traditionally authorized under national law are involved, without prejudice to points (a), (b) and (c).

3. In accordance with the Berne Convention for the protection of Literary and Artistic Works, this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder’s legitimate interests or conflicts with normal exploitation of the database.

CHAPTER III
SUI GENERIS RIGHT

Article 7
Object of protection

1. Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

2. For the purposes of this Chapter:

(a) ‘extraction’ shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;

(b) ‘re-utilization’ shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;

Public lending is not an act of extraction or re-utilization.

3. The right referred to in paragraph 1 may be transferred, assigned or granted under contractual licence.

4. The right provided for in paragraph 1 shall apply irrespective of the eligibility of that database for protection by copyright or by other rights. Moreover, it shall apply irrespective of eligibility of the contents of that database for protection by copyright or by other rights. Protection of databases under the right provided for in paragraph 1 shall be without prejudice to rights existing in respect of their contents.

5. The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted.

Article 8
Rights and obligations of lawful users

1. The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Where the lawful user is authorized to extract and/or re-utilize only part of the database, this paragraph shall apply only to that part.

2. A lawful user of a database which is made available to the public in whatever manner may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database.

3. A lawful user of a database which is made available to the public in any manner may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database.

Article 9
Exceptions to the sui generis right

Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents:

(a) in the case of extraction for private purposes of the contents of a non-electronic database;

(b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;

(c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

Article 10
Term of protection

1. The right provided for in Article 7 shall run from the date of completion of the making of the database. It shall expire fifteen years from the first of January of the year following the date of completion.

2. In the case of a database which is made available to the public in whatever manner before expiry of the period provided for in paragraph 1, the term of protection by that right shall expire fifteen years from the first of January of the year following the date when the database was first made available to the public.

3. Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.

Article 11
Beneficiaries of protection under the sui generis right

1. The right provided for in Article 7 shall apply to database whose makers or rightholders are nationals of a Member State or who have their habitual residence in the territory of the Community.

2. Paragraph 1 shall also apply to companies and firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Community; however, where such a company or firm has only its registered office in the territory of the Community, its operations must be genuinely linked on an ongoing basis with the economy of a Member State.

3. Agreements extending the right provided for in Article 7 to databases made in third countries and falling outside the provisions of paragraphs 1 and 2 shall be concluded by the Council acting on a proposal from the Commission. The term of any protection extended to databases by virtue of that procedure shall not exceed that available pursuant to Article 10.

CHAPTER IV
COMMON PROVISIONS

Article 12
Remedies

Member States shall provide appropriate remedies in respect of infringements of the rights provided for in this Directive.
Article 13

Continued application of other legal provisions

This Directive shall be without prejudice to provisions concerning in particular copyright, rights related to copyright or any other rights or obligations subsisting in the data, works or other materials incorporated into a database, patent rights, trade marks, design rights, the protection of national treasures, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, and the law of contract.

Article 14

Application over time

1. Protection pursuant to this Directive as regards copyright shall also be available in respect of databases created prior to the date referred to in Article 16 (1) which on that date fulfil the requirements laid down in this Directive as regards copyright protection of databases.

2. Notwithstanding paragraph 1, where a database protected under copyright arrangements in a Member State on the date of publication of this Directive does not fulfil the eligibility criteria for copyright protection laid down in Article 3 (1), this Directive shall not result in any curtailment in that Member State of the remaining term of protection afforded under those arrangements.

3. Protection pursuant to the provisions of this Directive as regards the right provided for in Article 7 shall also be available in respect of databases the making of which was completed not more than fifteen years prior to the date referred to in Article 16 (1) and which on that date fulfil the requirements laid down in Article 7.

4. The protection provided for in paragraphs 1 and 3 shall be without prejudice to any acts concluded and rights acquired before the date referred to in those paragraphs.

5. In the case of a database the making of which was completed not more than fifteen years prior to the date referred to in Article 16 (1), the term of protection by the right provided for in Article 7 shall expire fifteen years from the first of January following that date.

Article 15

Binding nature of certain provisions

Any contractual provision contrary to Articles 6 (1) and 8 shall be null and void.

Article 16

Final provisions

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 1 January 1998.

When Member States adopt these provisions, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field governed by this Directive.

3. Not later than at the end of the third year after the date referred to in paragraph 1, and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, in which, inter alia, on the basis of specific information supplied by the Member States, it shall examine in particular the application of the sui generis right, including Articles 8 and 9, and shall verify especially whether the application of this right has led to abuse of a dominant position or other interference with free competition which would justify appropriate measures being taken, including the establishment of non-voluntary licensing arrangements. Where necessary, it shall submit proposals for adjustment of this Directive in line with developments in the area of databases.

C-203/02 The British Horseracing Board Ltd and Others v William Hill Organization Ltd.

1. The expression ‘investment in ... the obtaining ... of the contents’ of a database in Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database.

The expression ‘investment in ... the ... verification ... of the contents’ of a database in Article 7(1) of Directive 96/9 must be understood to refer to the resources used, with a view to ensuring the reliability of the information contained in that database, to monitor the accuracy of the materials collected when the database was created and during its operation. The resources used for verification during the stage of creation of materials which are subsequently collected in a database do not fall within that definition.

The resources used to draw up a list of horses in a race and to carry out checks in that connection do not constitute investment in the obtaining and verification of the contents of the database in which that list appears.

2. The terms ‘extraction’ and ‘re-utilisation’ as defined in Article 7 of Directive 96/9 must be interpreted as referring to any unauthorised act of appropriation and distribution to the public of the whole or a part of the contents of a database. Those terms do not imply direct access to the database concerned.

The fact that the contents of a database were made accessible to the public by its maker or with his consent does not affect the right of the maker to prevent acts of extraction and/or re-utilisation of the whole or a substantial part of the contents of a database.

3. The expression ‘substantial part, evaluated quantitatively, of the contents of [a] database’ in Article 7 of Directive 96/9 refers to the volume of data extracted from the database and/or re-utilised and must be assessed in relation to the total volume of the contents of the database. The expression ‘substantial part, evaluated qualitatively ... of the contents of [a] database’ refers to the scale of the investment in the obtaining, verification or presentation of the contents of the subject of the act of extraction and/or re-utilisation, regardless of whether that subject represents a
quantitatively substantial part of the general contents of the protected database. Any part which does not fulfil the definition of a substantial part, evaluated both quantitatively and qualitatively, falls within the definition of an insubstantial part of the contents of a database.

4. The prohibition laid down by Article 7(5) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases refers to unauthorised acts of extraction or re-utilisation of the cumulative effect of which is to reconstitute and/or make available to the public, without the authorisation of the maker of the database, the whole or a substantial part of the contents of that database and thereby seriously prejudice the investment by the maker.

C-444/02 Fixtures Marketing Ltd v Organismos Prognostikon agionon podosfaistoro AE (OPAP)

The term ‘database’ as defined in Article 1(2) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases refers to any collection of works, data or other materials, separable from one another without the value of their contents being affected, including a method or system of some sort for the retrieval of each of its constituent materials. A fixture list for a football league such as that at issue in the case in the main proceedings constitutes a database within the meaning of Article 1(2) of Directive 96/9/EC.

The expression ‘investment in ... the obtaining ... of the contents’ of a database in Article 7(1) of Directive 96/9/EC must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database. In the context of drawing up a fixture list for the purpose of organising football league fixtures, therefore, it does not cover the resources used to establish the dates, times and the team pairings for the various matches in the league.

C-304/07 Directmedia Publishing GmbH v Albert-Ludwigs-Universität Freiburg

The transfer of material from a protected database to another database following an on-screen consultation of the first database and an individual assessment of the material contained in that first database is capable of constituting an ‘extraction’, within the meaning of Article 7 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, to the extent that – which it is for the referring court to ascertain – that operation amounts to the transfer of a substantial part of the material, evaluated qualitatively or quantitatively, of the contents of the protected database, or to transfers of insubstantial parts which, by their repeated or systematic nature, would have resulted in the reconstruction of a substantial part of those contents.

C-545/07 Apis-Hristovitch EOOD v Lakorda AD

1. The delimitation of the concepts of ‘permanent transfer’ and ‘temporary transfer’ in Article 7 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases is based on the criterion of the length of time during which materials extracted from a protected database are stored in a medium other than that database. The time at which there is an extraction, within the meaning of Article 7, from a protected database, accessible electronically, is when the materials which are the subject of the act of transfer are stored in a medium other than that database. The concept of extraction is independent of the objective pursued by the perpetrator of the act at issue, of any modifications he may make to the contents of the materials thus transferred, and of any differences in the structural organisation of the databases concerned.

The fact that the physical and technical characteristics present in the contents of a protected database made by a particular person also appear in the contents of a database made by another person may be interpreted as evidence of extraction within the meaning of Article 7 of Directive 96/9/EC, unless that coincidence can be explained by factors other than a transfer between the two databases concerned. The fact that materials obtained by the maker of a database from sources not accessible to the public also appear in a database made by another person is not sufficient, in itself, to prove the existence of such extraction but can constitute circumstantial evidence thereof.

The nature of the computer program used to manage two electronic databases is not a factor in assessing the existence of extraction within the meaning of Article 7 of Directive 96/9/EC.

2. Article 7 of Directive 96/9/EC must be interpreted as meaning that, where there is a body of materials composed of separate modules, the volume of those materials allegedly extracted and/or re-utilised from one of those modules must, in order to assess whether there has been extraction and/or re-utilisation of a substantial part, evaluated quantitatively, of the contents of a database within the meaning of that article, be compared with the total contents of that module. If the latter constitutes, in itself, a database which fulfils the conditions for protection by the sui generis right. Otherwise, and in so far as the body of materials constitutes a database protected by that right, the comparison must be made between the volume of the materials allegedly extracted and/or re-utilised from the various modules of that database and its total contents.

The fact that the materials allegedly extracted and/or re-utilised from a database protected by the sui generis right were obtained by the maker of that database from sources not accessible to the public may, according to the amount of human, technical and/or financial resources deployed by the maker to collect the materials at issue from those sources, affect the classification of those materials as a substantial part, evaluated qualitatively, of the contents of the database concerned, within the meaning of Article 7 of Directive 96/9/EC.

The fact that part of the materials contained in a database are official and accessible to the public does not relieve the national court of an obligation, in assessing whether there has been extraction and/or re-utilisation of a substantial part of the contents of that database, to verify whether the materials allegedly extracted and/or re-utilised from that database constitute a substantial part, evaluated quantitatively, of its contents or, as the case may be, whether they constitute a substantial part, evaluated qualitatively, of the database insomuch as they represent, in terms of the obtaining, verification and presentation thereof, a substantial human, technical or financial investment.

C-338/02 Fixtures Marketing Ltd v Svenska Spel AB

The expression ‘investment in ... the obtaining ... of the contents’ of a database in Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database. In the context of drawing up a fixture list for the purpose of organising football league fixtures, therefore, it does not cover the resources used to establish the dates, times and the team pairings for the various matches in the league.

C-604/10 Football Dataco Ltd and Others v Yahoo! UK Limited and Others

1. Article 3(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be interpreted as meaning that a ‘database’ within the meaning of Article 1(2) of that directive is protected by the copyright laid down by that directive
provided that the selection or arrangement of the data which it contains amounts to an original expression of the creative freedom of its author, which is a matter for the national court to determine.

As a consequence:
- the intellectual effort and skill of creating that data are not relevant in order to assess the eligibility of that database for protection by that right;
- it is irrelevant, for that purpose, whether or not the selection or arrangement of that data includes the addition of important significance to that data, and
- the significant labour and skill required for setting up that database cannot as such justify such a protection if they do not express any originality in the selection or arrangement of the data which that database contains.

2. Directive 96/9 must be interpreted as meaning that, subject to the transitional provision contained in Article 14(2) of that directive, it precludes national legislation which grants databases, as defined in Article 1(2) of the directive, copyright protection under conditions which are different to those set out in Article 3(1) of the directive.

**C-202/12 Innowebo BV v Wegener ICT Media BV, Wegener Mediaventions BV**

Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be interpreted as meaning that an operator who makes available on the Internet a dedicated meta search engine such as that at issue in the main proceedings re-utilises the whole or a substantial part of a database protected under Article 7, where that dedicated meta engine:

- provides the end user with a search form which essentially offers the same range of functionality as the search form on the database site:
- 'translates' queries from end users into the search engine for the database site 'in real time', so that all the information on that database is searched through and
- presents the results to the end user using the format of its website, grouping duplications together into a single block item but in an order that reflects criteria comparable to those used by the search engine of the database site concerned for presenting results.


**Article 1 – Subject matter**

This Directive concerns the measures, procedures and remedies necessary to ensure the enforcement of intellectual property rights. For the purposes of this Directive, the term ‘intellectual property rights’ includes industrial property rights.

**Article 2 – Scope**

1. Without prejudice to the means which are or may be provided for in Community or national legislation, in so far as those means may be more favourable for rightholders, the measures, procedures and remedies provided for by this Directive shall apply, in accordance with Article 3, to any infringement of intellectual property rights as provided for by Community law and/or by the national law of the Member State concerned.

2. This Directive shall be without prejudice to the specific provisions on the enforcement of rights and on exceptions contained in Community legislation concerning copyright and rights related to copyright, notably those found in Directive 91/250/EEC and, in particular, Articles 7 thereof; in Directive 2001/29/EC and, in particular, Articles 2 to 6 and Article 8 thereof.

3. This Directive shall not affect:

(a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;

(b) Member States’ international obligations and notably the TRIPS Agreement, including those relating to criminal procedures and penalties;

(c) any national provisions in Member States relating to criminal procedures or penalties in respect of infringement of intellectual property rights.

**CHAPTER II MEASURES, PROCEDURES AND REMEDIES**

**Section 1 General provisions**

**Article 3 – General obligation**

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. These measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.

**Article 4 – Persons entitled to apply for the application of the measures, procedures and remedies**
Member States shall recognise as persons entitled to seek application of the measures, procedures and remedies referred to in this chapter:

(a) the holders of intellectual property rights, in accordance with the provisions of the applicable law;
(b) all other persons authorised to use those rights, in particular licensees, in so far as permitted by and in accordance with the provisions of the applicable law;
(c) intellectual property collective rights-management bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law;
(d) professional defence bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law.

**Article 5 – Presumption of authorship or ownership**

For the purposes of applying the measures, procedures and remedies provided for in this Directive, (a) for the author of a literary or artistic work, in the absence of proof to the contrary, to be regarded as such, and consequently to be entitled to institute infringement proceedings, it shall be sufficient for his/her name to appear on the work in the usual manner;
(b) the provision under (a) shall apply mutatis mutandis to the holders of rights related to copyright with regard to their protected subject matter.

**Section 2**

**Evidence**

**Article 6 – Evidence**

1. Member States shall ensure that, on application by a party which has presented reasonably available evidence sufficient to support its claims, and has, in substantiating those claims, specified evidence which lies in the control of the opposing party, the competent judicial authorities may order that such evidence be presented by the opposing party, subject to the protection of confidential information. For the purposes of this paragraph, Member States may provide that a reasonable sample of a substantial number of copies of a work or any other protected object be considered by the competent judicial authorities to constitute reasonable evidence.

2. Under the same conditions, in the case of an infringement committed on a commercial scale Member States shall take such measures as are necessary to enable the competent judicial authorities to order, where appropriate, on application by a party, the communication of banking, financial or commercial documents under the control of the opposing party, subject to the protection of confidential information.

**Article 7 – Measures for preserving evidence**

1. Member States shall ensure that, even before the commencement of proceedings on the merits of the case, the competent judicial authorities may, on application by a party who has presented reasonably available evidence to support his/her claims that his/her intellectual property right has been infringed or is about to be infringed, order prompt and effective provisional measures to preserve relevant evidence in respect of the alleged infringement, subject to the protection of confidential information.

Such measures may include the detailed description, with or without the taking of samples, or the physical seizure of the infringing goods, and, in appropriate cases, the materials and implements used in the production and/or distribution of these goods and the documents relating thereto. Those measures shall be taken, if necessary without the other party having been heard, in particular where any delay is likely to cause irreparable harm to the rightholder or where there is a demonstrable risk of evidence being destroyed.

Where measures to preserve evidence are adopted without the other party having been heard, the parties affected shall be given notice, without delay after the execution of the measures at the latest. A review, including a right to be heard, shall take place upon request of the parties affected with a view to deciding within a reasonable period after the notification of the measures, whether the measures shall be modified, revoked or confirmed.

2. Member States shall ensure that the measures to preserve evidence may be subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the defendant as provided for in paragraph 4.

3. Member States shall ensure that the measures to preserve evidence are revoked or otherwise cease to have effect, upon request of the defendant, without prejudice to the damages which may be claimed, if the applicant does not institute, within a reasonable period, proceedings leading to a decision on the merits of the case before the competent judicial authority, the period to be determined by the judicial authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer.

4. Where the measures to preserve evidence are revoked, or where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no infringement or threat of infringement of an intellectual property right, the judicial authorities shall have the authority to order the applicant, upon request of the defendant, to provide the defendant appropriate compensation for any injury caused by those measures.

5. Member States may take measures to protect witnesses' identity.

**Section 3**

**Right of information**

**Article 8 – Right of information**

1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:
(a) was found in possession of the infringing goods on a commercial scale;
(b) was found to be using the infringing services on a commercial scale;
(c) was found to be providing on a commercial scale services which infringe an intellectual property right;
(d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.

2. The information referred to in paragraph 1 shall, as appropriate, comprise:
Section 4
Provisional and precautionary measures

Article 9 - Provisional and precautionary measures

1. Member States shall ensure that the judicial authorities may, at the request of the applicant:
   (a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the rightholder; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe a copyright or a related right so as to prevent their entry into or movement within the channels of commerce.
   (b) order the seizure or delivery up of the goods suspected of infringing an intellectual property right so as to prevent their entry into or movement within the channels of commerce;
   (c) destruction.

2. The judicial authorities shall order that those measures be carried out at the expense of the infringer, unless particular circumstances prevalent in the case make it necessary to order the rightholder to pay the costs.

3. In the course of the infringement committed on a commercial scale, the Member States shall ensure that, if the injured party demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of his/her bank accounts and other assets. To that end, the competent authorities may order the communication of bank, financial or commercial documents, or appropriate access to the relevant information.

4. The judicial authorities shall, in respect of the measures referred to in paragraphs 1 and 2, have the authority to require the applicant to provide any reasonably available evidence in order to satisfy themselves with a sufficient degree of certainty that the applicant is the rightholder and that the applicant's right is being infringed, or that such infringements are imminent.

5. Member States shall ensure that the provisional measures referred to in paragraphs 1 and 2 are revoked or otherwise cease to have effect, upon request of the defendant, if the applicant does not institute, within a reasonable period, proceedings leading to a decision on the merits of the case before the competent judicial authority, the period to be determined by the judicial authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer.

6. The competent judicial authorities may make the provisional measures referred to in paragraphs 1 and 2 subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the defendant as provided for in paragraph 7.

7. Where the provisional measures are revoked or where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no infringement or threat of infringement of an intellectual property right, the judicial authorities shall have the authority to order the defendant, upon request of the applicant, to provide the defendant appropriate compensation for any injury caused by those measures.

Section 5
Measures resulting from a decision on the merits of the case

Article 10 - Corrective measures

1. Without prejudice to any damages due to the rightholder by reason of the infringement, and without compensation of any sort, Member States shall ensure that the competent judicial authorities may order, at the request of the applicant, that appropriate measures be taken with regard to goods that have been found to be infringing an intellectual property right and, in appropriate cases, with regard to materials and implements principally used in the creation or manufacture of those goods. Such measures shall include:
   (a) recall from the channels of commerce;
   (b) definitive removal from the channels of commerce; or
   (c) destruction.

2. The judicial authorities shall order that those measures be carried out at the expense of the infringer, unless particular reasons are invoked for not doing so.

3. In considering a request for corrective measures, the need for proportionality between the seriousness of the infringement and the remedies ordered as well as the interests of third parties shall be taken into account.

Article 11 - Injunctions

Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.

Article 12 - Alternative measures
Member States may provide that, in appropriate cases and at the request of the person liable to be subject to the measures provided for in this section, the competent judicial authorities may order pecuniary compensation to be paid to the injured party instead of applying the measures provided for in this section if that person acted unintentionally and without negligence, if execution of the measures in question would cause him/her disproportionate harm and if pecuniary compensation to the injured party appears reasonably satisfactory.

**Section 6**

**Damages and legal costs**

**Article 13 – Damages**

1. Member States shall ensure that the competent judicial authorities, on application of the injured party, order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the rightholder damages appropriate to the actual prejudice suffered by him/her as a result of the infringement.

When the judicial authorities set the damages:

(a) they shall take into account all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the rightholder by the infringer;

or

(b) as an alternative to (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question.

2. Where the infringer did not knowingly, or with reasonable grounds to know, engage in infringing activity, Member States may lay down that the judicial authorities may order the recovery of profits or the payment of damages, which may be pre-established.

**Article 14 – Legal costs**

Member States shall ensure that reasonable and proportionate legal costs and other expenses incurred by the successful party shall, as a general rule, be borne by the unsuccessful party, unless equity does not allow this.

**Section 7**

**Publicity measures**

**Article 15 – Publication of judicial decisions**

Member States shall ensure that, in legal proceedings instituted for infringement of an intellectual property right, the judicial authorities may order, at the request of the applicant and at the expense of the infringer, appropriate measures for the dissemination of the information concerning the decision, including displaying the decision and publishing it in full or in part. Member States may provide for other additional publicity measures which are appropriate to the particular circumstances, including prominent advertising.

**CHAPTER III**

**SANCTIONS BY MEMBER STATES**

**Article 16 – Sanctions by Member States**

Without prejudice to the civil and administrative measures, procedures and remedies laid down by this Directive, Member States may apply other appropriate sanctions in cases where intellectual property rights have been infringed.

**CHAPTER IV**

**CODES OF CONDUCT AND ADMINISTRATIVE COOPERATION**

**Article 17 – Codes of conduct**

Member States shall encourage:

(a) the development by trade or professional associations or organisations of codes of conduct at Community level aimed at contributing towards the enforcement of the intellectual property rights, particularly by recommending the use on optical discs of a code enabling the identification of the origin of their manufacture;

(b) the submission to the Commission of draft codes of conduct at national and Community level and of any evaluations of the application of these codes of conduct.

**Article 18 – Assessment**

1. Three years after the date laid down in Article 20(1), each Member State shall submit to the Commission a report on the implementation of this Directive. On the basis of those reports, the Commission shall draw up a report on the application of this Directive, including an assessment of the effectiveness of the measures taken, as well as an evaluation of its impact on innovation and the development of the information society. That report shall then be transmitted to the European Parliament, the Council and the European Economic and Social Committee. It shall be accompanied, if necessary and in the light of developments in the Community legal order, by proposals for amendments to this Directive.

2. Member States shall provide the Commission with all the aid and assistance it may need when drawing up the report referred to in the second subparagraph of paragraph 1.

**Article 19 – Exchange of information and correspondents**

For the purpose of promoting cooperation, including the exchange of information, among Member States and between Member States and the Commission, each Member State shall designate one or more national correspondents for any question relating to the implementation of the measures provided for by this Directive. It shall communicate the details of the national correspondent(s) to the other Member States and to the Commission.

**CHAPTER V**

**FINAL PROVISIONS**

**Article 20 – Implementation**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 29 April 2006. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.
This Directive shall enter into force on the 20th day following that of its publication in the Official Journal of the European Union.

---

Article 21 – Entry into force

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:


(2) The Berne Convention for the protection of literary and artistic works and the International Convention for the protection of performers, producers of phonograms and broadcasting organisations (Rome Convention) lay down only minimum terms of protection of the rights they refer to, leaving the Contracting States free to grant longer terms.

(3) Certain Member States have exercised this entitlement. In addition, some Member States have not yet become party to the Rome Convention.

(4) It is important to lay down not only the terms of protection as such, but also certain implementing arrangements, such as the date from which each term of protection is calculated.

(5) The provisions of this Directive should not affect the application by the Member States of the provisions of Article 14 bis (2)(b), (c) and (d) and (3) of the Berne Convention.

(6) The minimum term of protection laid down by the Berne Convention, namely the life of the author and 50 years after his death, was intended to provide protection for the author and the first two generations of his descendants. The average lifespan in the Community has grown longer, to the point where this term is no longer sufficient to cover two generations.

(7) Certain Member States have granted a term longer than 50 years after the death of the author in order to offset the effects of the world wars on the exploitation of authors’ works.

(8) For the protection of related rights certain Member States have introduced a term of 50 years after lawful publication or lawful communication to the public.

(9) The Diplomatic Conference held in December 1996, under the auspices of the World Intellectual Property Organization (WIPO), led to the adoption of the WIPO Performances and Phonograms Treaty, which deals with the protection of performers and producers of phonograms. This Treaty took the form of a substantial up-date of the international protection of related rights.

(10) Due regard for established rights is one of the general principles of law protected by the Community legal order. Therefore, the terms of protection of copyright and related rights established by Community law cannot have the effect of reducing the protection enjoyed by rightholders in the Community before the entry into force of Directive 93/98/EEC. In order to keep the effects of transitional measures to a minimum and to allow the internal market to function smoothly, those terms of protection should be applied for long periods.

(11) The level of protection of copyright and related rights should be high, since those rights are fundamental to intellectual creation. Their protection ensures the maintenance and development of creativity in the interest of authors, cultural industries, consumers and society as a whole.

(12) In order to establish a high level of protection which at the same time meets the requirements of the internal market and the need to establish a legal environment conducive to the harmonious development of literary and artistic creation in the Community, the term of protection for copyright should be harmonised at 70 years after the death of the author or 70 years after the work is lawfully made available to the public, and for related rights at 50 years after the event which sets the term running.

(13) Collectors are protected according to Article 2(5) of the Berne Convention when, by reason of the selection and arrangement of their content, they constitute intellectual creations. Those works are protected as such, without prejudice to the copyright in each of the works forming part of such collections. Consequently, specific terms of protection may apply to works included in collections.

(14) In all cases where one or more physical persons are identified as authors, the term of protection should be calculated after their death. The question of authorship of the whole or a part of a work is a question of fact which the national courts may have to decide.

(15) Terms of protection should be calculated from the first day of January of the year following the relevant event, as they are in the Berne and Rome Conventions.

(16) The protection of photographs in the Member States is the subject of varying regimes. A photographic work within the meaning of the Berne Convention is to be considered original if it is the author’s own intellectual creation reflecting his personality, no other criteria such as merit or purpose being taken into account. The protection of other photographs should be left to national law.

(17) In order to avoid differences in the term of protection as regards related rights it is necessary to provide the same starting point for the calculation of the term throughout the Community. The performance, fixation, transmission, lawful publication, and lawful communication to the public, that is to say the means of making a subject of a related right perceptible in all appropriate ways to persons in general, should be taken into account for the calculation of the term of protection regardless of the country where this performance,
(18) The rights of broadcasting organisations in their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite, should not be perpetual. It is therefore necessary to have the term of protection running from the first transmission of a particular broadcast only. This provision is understood to avoid a new term running in cases where a broadcast is identical to a previous one.

(19) The Member States should remain free to maintain or introduce other rights related to copyright in particular in relation to the protection of critical and scientific publications. In order to ensure transparency at Community level, it is however necessary for Member States which introduce new related rights to notify the Commission.

(20) It should be made clear that this Directive does not apply to moral rights.

(21) For works whose country of origin within the meaning of the Berne Convention is a third country and whose author is not a Community national, the same provisions of this Directive shall apply, provided that the term accorded in the Community does not exceed the term laid down in this Directive.

(22) Where a rightholder who is not a Community national qualifies for protection under an international agreement, the term of protection of related rights should be the same as that laid down in this Directive. However, this term should not exceed that fixed in the third country of which the rightholder is a national.

(23) Comparison of terms should not result in Member States being brought into conflict with their international obligations.

(24) Member States should remain free to adopt provisions on the interpretation, adaptation and further execution of contracts on the exploitation of protected works and other subject matter which were concluded before the extension of the term of protection resulting from this Directive.

(25) Respect of acquired rights and legitimate expectations is part of the Community legal order. Member States may provide in particular that in certain circumstances the copyright and related rights which are revived pursuant to this Directive may not give rise to payments by persons who undertook in good faith the exploitation of the works at the time when such works lay within the public domain.

(26) This Directive should be without prejudice to the obligations of the Member States relating to the time-limits for transposition into national law and application of the Directives, as set out in Part B of Annex I.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Duration of authors' rights

1. The rights of an author of a literary or artistic work within the meaning of Article 2 of the Berne Convention shall run for the life of the author and for 70 years after his death, irrespective of the date when the work is lawfully made available to the public.

2. In the case of a work of joint authorship, the term referred to in paragraph 1 shall be calculated from the death of the last surviving author.

3. In the case of anonymous or pseudonymous works, the term of protection shall run for 70 years after the work is lawfully made available to the public. However, when the pseudonym adopted by the author leaves no doubt as to his identity, or if the author discloses his identity during the period referred to in the first sentence, the term of protection applicable shall be that laid down in paragraph 1.

4. Where a Member State provides for particular provisions on copyright in respect of collective works or for a legal person to be designated as the rightholder, the term of protection shall be calculated according to the provisions of paragraph 3, except if the natural persons who have created the work are identified as such in the versions of the work which are made available to the public. This paragraph is without prejudice to the rights of identified authors whose identifiable contributions are included in such works, to which contributions paragraph 1 or 2 shall apply.

5. Where a work is published in volumes, parts, instalments, issues or episodes and the term of protection runs from the time when the work was lawfully made available to the public, the term of protection shall run for each such item separately.

6. In the case of works for which the term of protection is not calculated from the death of the author or authors and which have not been lawfully made available to the public within 70 years from their creation, the protection shall terminate.

7. The term of protection of a musical composition with words shall expire 70 years after the death of the last of the following persons to survive, whether or not those persons are designated as co-authors: the author of the lyrics and the composer of the musical composition, provided that both contributions were specifically created for the respective musical composition with words.

Article 2

Cinematographic or audiovisual works

1. The principal director of a cinematographic or audiovisual work shall be considered as its author or one of its authors. Member States shall be free to designate other co-authors.

2. The term of protection of cinematographic or audiovisual works shall expire 70 years after the death of the last of the following persons to survive, whether or not these persons are designated as co-authors: the author of the screenplay, the author of the dialogue and the composer of the musical composition, provided that both contributions were specifically created for use in the cinematographic or audiovisual work.

Article 3

Duration of related rights

1. The rights of performers shall expire 50 years after the date of the performance. However, if a fixation of the performance is lawfully published or lawfully communicated to the public within this period, the rights shall expire 50 years from the date of the first such publication or the first such communication to the public, whichever is the earlier.

However, — if a fixation of the performance otherwise than in a phonogram is lawfully published or lawfully communicated to the public within this period, the rights shall expire 50 years from the date of the first such publication or the first such communication to the public, whichever is the earlier.

— if a fixation of the performance in a phonogram is lawfully published or lawfully communicated to the public within this period, the rights shall expire 70 years from the date of the first such publication or the first such communication to the public, whichever is the earlier.

2. The rights of producers of phonograms shall expire 50 years after the fixation is made. However, if the phonogram has been lawfully published within this period, the said rights shall expire 70 years from the date of the first lawful publication. If no lawful publication has taken place within the period mentioned in the first sentence, and if the phonogram has been lawfully communicated to the public within this period, the said rights shall expire 70 years from the date of the first lawful communication to the public.

2a. If, 50 years after the phonogram was lawfully published or, failing such publication, 50 years after it was lawfully communicated to the public, the phonogram producer does not offer copies of the phonogram for sale in sufficient quantity or does not make it available to the public, by wire or wireless means, in such a way that members of the public may access it from a place and at a time individually chosen by them, the performer may terminate the contract by which the
performer has transferred or assigned his rights in the fixation of his performance to a phonogram producer (hereinafter a 'contract on transfer or assignment'). The right to terminate the contract on transfer or assignment may be exercised if the producer, within a year from the notification by the performer of his intention to terminate the contract on transfer or assignment pursuant to the previous sentence, fails to carry out both of the acts of exploitation referred to in that sentence. This right to terminate may not be waived by the performer. Where a phonogram contains the fixation of the performances of a plurality of performers, they may terminate their contracts on transfer or assignment in accordance with applicable national law. If the contract on transfer or assignment is terminated pursuant to this paragraph, the rights of the phonogram producer in the phonogram shall expire.

2b. Where a contract on transfer or assignment gives the performer a right to claim a non-recurring remuneration, the performer shall have the right to obtain an annual supplementary remuneration from the phonogram producer for each full year immediately following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public. The right to obtain such annual supplementary remuneration may not be waived by the performer.

2c. The overall amount to be set aside by a phonogram producer for payment of the annual supplementary remuneration referred to in paragraph 2b shall correspond to 20 % of the revenue which the phonogram producer has derived, during the year preceding that for which the said remuneration is paid, from the reproduction, distribution and making available of the phonogram in question, following the 50th year after it was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public.

Member States shall ensure that phonogram producers are required on request to provide to performers who are entitled to the annual supplementary remuneration referred to in paragraph 2b any information which may be necessary in order to secure payment of that remuneration.

2d. Member States shall ensure that the right to obtain an annual supplementary remuneration as referred to in paragraph 2b is administered by collecting societies.

2e. Where a performer is entitled to recurring payments, neither advance payments nor any contractually defined deductions shall be deducted from the payments made to the performer following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public.

3. The rights of producers of the first fixation of a film shall expire 50 years from the date of the first such fixation or the first such communication to the public, whichever is the earlier. The term 'film' shall designate a cinematographic or audiovisual work or moving images, whether or not accompanied by sound.

4. The rights of broadcasting organisations shall expire 50 years after the first transmission of a broadcast, whether this broadcast is transmitted by wire or over the air, including by cable or satellite.

Article 4
Protection of previously unpublished works
Any person who, after the expiry of copyright protection, for the first time lawfully publishes or lawfully communicates to the public a previously unpublished work, shall benefit from a protection equivalent to the economic rights of the author. The term of protection of such rights shall be 25 years from the time when the work was first lawfully published or lawfully communicated to the public.

Article 5
Critical and scientific publications
Member States may protect critical and scientific publications of works which have come into the public domain. The maximum term of protection of such rights shall be 30 years from the time when the publication was first lawfully published.

Article 6
Protection of photographs
Photographs which are original in the sense that they are the author's own intellectual creation shall be protected in accordance with Article 1. No other criteria shall be applied to determine their eligibility for protection. Member States may provide for the protection of other photographs.

Article 7
Protection vis-à-vis third countries
1. Where the country of origin of a work, within the meaning of the Berne Convention, is a third country, and the author of the work is not a Community national, the term of protection granted by the Member States shall expire on the date of expiry of the protection granted in the country of origin of the work, but may not exceed the term laid down in Article 1.

2. The terms of protection laid down in Article 3 shall also apply in the case of rightholders who are not Community nationals, provided Member States grant them protection. However, without prejudice to the international obligations of the Member States, the term of protection granted by Member States shall expire no later than the date of expiry of the protection granted in the country of which the rightholder is a national and may not exceed the term laid down in Article 3.

3. Member States which, on 29 October 1993, in particular pursuant to their international obligations, granted a longer term of protection than that which would result from the provisions of paragraphs 1 and 2 may maintain this protection until the conclusion of international agreements on the term of protection of copyright or related rights.

Article 8
Calculation of terms
The terms laid down in this Directive shall be calculated from the first day of January of the year following the event which gives rise to them.

Article 9
Moral rights
This Directive shall be without prejudice to the provisions of the Member States regulating moral rights.

Article 10
Application in time
1. Where a term of protection which is longer than the corresponding term provided for by this Directive was already running in a Member State on 1 July 1995, this Directive shall not have the effect of shortening that term of protection in that Member State.

2. The terms of protection provided for in this Directive shall apply to all works and subject matter which were protected in at least one Member State on the date referred to in paragraph 1, pursuant to national provisions on copyright or related rights, or which meet the criteria for protection under [Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property] (5).

3. This Directive shall be without prejudice to any acts of exploitation performed before the date referred to in paragraph 1. Member States shall adopt the necessary provisions to protect in particular acquired rights of third parties.

4. Member States need not apply the provisions of Article 2(1) to cinematographic or audiovisual works created before 1 July 1994.

5. Article 3(1) to (2e) in the version thereof in force on 31 October 2011 shall apply to fixations of performances and
phonograms in regard to which the performer and the phonogram producer are still protected, by virtue of those provisions in the version thereof in force on 30 October 2011, as at 1 November 2013 and to fixations of performances and phonograms which come into being after that date.

6. Article 1(7) shall apply to musical compositions with words of which at least the musical composition or the lyrics are protected in at least one Member State on 1 November 2013, and to musical compositions with words which come into being after that date.

The first subparagraph of this paragraph shall be without prejudice to any acts of exploitation performed before 1 November 2013. Member States shall adopt the necessary provisions to protect, in particular, acquired rights of third parties.

Article 10a
Transitional measures
1. In the absence of clear contractual indications to the contrary, a contract on transfer or assignment concluded before 1 November 2013 shall be deemed to continue to produce its effects beyond the moment at which, by virtue of Article 3(1) in the version thereof in force on 30 October 2011, the performer would no longer be protected.

2. Member States may provide that contracts on transfer or assignment which entitle a performer to recurring payments and which are concluded before 1 November 2013 can be modified following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public.

Article 11
Notification and communication
1. Member States shall immediately notify the Commission of any governmental plan to grant new related rights, including the basic reasons for their introduction and the term of protection envisaged.
2. Member States shall communicate to the Commission the texts of the provisions of internal law which they adopt in the field governed by this Directive.

[---]

Article 13
Entry into force
This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
VIII. Electronic documents


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof;

Having regard to the proposal from the Commission (1);

Having regard to the opinion of the Economic and Social Committee (2);

Having regard to the opinion of the Committee of the Regions (3);

Acting in accordance with the procedure laid down in Article 251 of the Treaty (4);

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication — towards a European framework for digital signatures and encryption;

(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;

(4) Electronic communication and commerce necessitate electronic signatures and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods (5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods (6);

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;

(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and
businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;

(13) Member States may decide how they ensure to comply with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to be supervised under any applicable accreditation scheme;

(14) It is important to strike a balance between consumer and business needs;

(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;

(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;

(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;

(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;

(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;

(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (7);

(27)
Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective.

HAVE ADOPTED THIS DIRECTIVE:

Article 1 Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2 Definitions

For the purpose of this Directive:
1. ‘electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. ‘signatory’ means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. ‘signature-creation data’ means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. ‘signature-creation device’ means configured software or hardware used to implement the signature-creation data;
6. ‘secure-signature-creation device’ means a signature-creation device which meets the requirements laid down in Annex III;
7. ‘signature-verification-data’ means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. ‘signature-verification device’ means configured software or hardware used to implement the signature-verification data;
9. ‘certificate’ means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. ‘qualified certificate’ means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;
11. ‘certification-service-provider’ means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
12. ‘electronic-signature product’ means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
13. ‘voluntary accreditation’ means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3 Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.
2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.
3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.
4. ►M1 The conformity of secure signature-creation devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall establish criteria for Member States to determine whether a body should be so designated. That measure, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 9(3). ◄

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.
5. The Commission may, in accordance with the procedure laid down ►M1 in Article 9(2) ◄, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.
6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

Article 4 Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-
service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
   (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
   (b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
   (a) in electronic form, or
   (b) not based upon a qualified certificate, or
   (c) not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
   (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
   (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
   (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
   1. unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.


Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
   (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
   (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
   (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements between the Community and third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (9).

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

▼M1

Article 9

Committee procedure

1. The Commission shall be assisted by the Electronic-Signature Committee.
2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period provided for in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

▼B

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:
(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
(c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 15

Addressees

This Directive is addressed to the Member States.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:
(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the signatory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:
(a) demonstrate the reliability necessary for providing certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of
the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:
— only authorised persons can make entries and changes,
— information can be checked for authenticity,
— certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
— any technical changes compromising these security requirements are apparent to the operator.

ANNEX III
Requirements for secure signature-creation devices
1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV
Recommendations for secure signature verification
During the signature-verification process it should be ensured with reasonable certainty that:
(a) the data used for verifying the signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of that verification is correctly displayed;
(c) the verifier can, as necessary, reliably establish the contents of the signed data;
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
(e) the result of verification and the signatory's identity are correctly displayed;
(f) the use of a pseudonym is clearly indicated; and
(g) any security-relevant changes can be detected.

Amended by:


(2003/511/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,
Having regard to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(1), and in particular Article 3(5) thereof,

Whereas:

(1)

(2) The task of drawing up the technical specifications needed for the production and placing on the market of products taking into account the current stage of technology, is carried out by organisations competent in the standardisation area.

(3) CEN (European Committee for Standardisation) and ETSI (European Telecommunications Standards Institute) within EESSI (European Electronic Signature Standardisation Initiative) are offering an open, inclusive and flexible European platform for consensus building in support of the development of the Information Society in Europe. They have developed standards for electronic signature products (CWA-CEN workshop agreement and ETSI TS-ETSI technical specification) on the basis of the requirements of the Annexes to Directive 1999/93/EC.

(4) The measures provided for in this decision are in accordance with the opinion of the "Electronic Signature Committee", HAS ADOPTED THIS DECISION:

Article 1
Reference numbers of generally recognised standards for electronic signature products are laid down in the Annex.

Article 2
The Commission shall review the operation of this Decision within two years from the date of its publication in the Official Journal of the European Union and report to the Committee established under Article 9(1) of Directive 1999/93/EC.

Article 3
This Decision is addressed to the Member States.

Done at Brussels, 14 July 2003.
For the Commission
Erkki Liikanen
Member of the Commission


ANNEX
A. List of generally recognised standards for electronic signature products that Member States shall presume are in compliance with the requirements laid down in Annex II f to Directive 1999/93/EC

B. List of the generally recognised standards for electronic signature products that Member States shall presume are in compliance with the requirements laid down in Annex III to Directive 1999/
HAS ADOPTED THIS DECISION:

Article 1

The purpose of this Decision is to establish the criteria for Member States to determine whether a national body should be designated as responsible for the conformity assessments of secure signature-creation-devices.

Article 2

Where a designated body is part of an organisation involved in activities other than conformance assessment of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC it must be identifiable within that organisation. Different activities must be clearly distinguished.

Article 3

The body and its staff must not engage in any activities that may conflict with their independence of judgement and integrity in relation to their task. In particular, the body must be independent of the parties involved. Therefore, the body, its executive officer and the staff responsible for carrying out the conformance assessment tasks must not be a designer, manufacturer, supplier or installer of secure signature-creation-devices, or a certification service provider issuing certificates to the public, nor the authorised representative of any of such parties. In addition, they must be financially independent and not become directly involved in the design, construction, marketing or maintenance of secure signature-creation-devices, nor represent the parties engaged in these activities. This does not preclude the possibility of exchange of technical information between the manufacturer and the designated body.

Article 4

The body and its personnel must be able to determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC with a high degree of professional integrity, reliability and sufficient technical competence.

Article 5

The body shall be transparent in its conformity assessment practices and shall record all relevant information concerning these practices. All interested parties must have access to the services of the body. The procedures under which the body operates must be administered in a non-discriminatory manner.

Article 6

The body must have at its disposal the necessary staff and facilities to enable it to perform properly and swiftly the technical and administrative work associated with the task for which it has been designated.

Article 7

The personnel responsible for conformity assessment must have:

- sound technical and vocational training, particularly in the field of electronic signature technologies and the related IT security aspects,
- satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate experience to carry out such assessments.

Article 8

The impartiality of staff shall be guaranteed. Their remuneration shall not depend on the number of conformity assessments carried out nor on the results of such conformity assessments.

Article 9

The body must have adequate arrangements to cover liabilities arising from its activities, for example, by obtaining appropriate insurance.

Article 10

The body must have adequate arrangements to ensure the confidentiality of the information obtained in carrying out its tasks under Directive 1999/93/EC or any provision of national law giving effect thereto, except vis-a-vis the competent authorities of the designating Member State.

Article 11

Where a designated body arranges for the carrying out of a part of the conformity assessments by another party, it must ensure and be able to demonstrate that this party is competent to perform the service in question. The designated body must take full responsibility for the work carried out under those arrangements. The final decision remains with the designated body.

Article 12

This Decision is addressed to the Member States.

Done at Brussels, 6 November 2000.

For the Commission

Erkki Liikanen
Member of the Commission


The European Parliament and the Council of the European Union

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.


(4) The Commission communication of 26 August 2010 entitled ‘A Digital Agenda for Europe’ identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled ‘Dismantling the obstacles to EU citizens’ rights’, the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

(5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.

(7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce (4), stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

(8) Directive 2006/123/EC of the European Parliament and of the Council (5) requires Member States to establish ‘points of single contact’ (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

(9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

(10) Directive 2011/24/EU of the European Parliament and of the Council (6) set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting ‘common identification and authentication measures to facilitate transferability of data in cross-border healthcare’. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.

(11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (7). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

(12) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identification management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

(13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.

(14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other’s electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State’s electronic identification scheme meets the conditions of notification and the notification was published in the Official Journal of the European Union.
However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.

(15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the person seeking to be identified is physically present or when the means are in electronic form.

(16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various techniques, processes and description may exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technolog-neutral. It should be possible to achieve the necessary security requirements through different technologies.

(17) Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online service or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established within the territory of that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme are presently available to private sector relying parties.

(18) This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

(19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless, technical requirements resulting from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.

(20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.

(21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should the Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.

(23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.

(24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.

(25) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.

(26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.

(27) This Regulation should be technolog-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-
level security of whatever qualified trust services and products are used or provided.

(29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/49/EC (8), in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.

(30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

(32) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users’ trust in the single market.

(33) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.

(34) All Member States should follow common essential supervisory requirements to ensure a comparable level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(35) All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

(36) Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of personal data within the internal market. Non-qualified trust service providers should be subject to a light touch and reactive ex post supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.

(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognizable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

(38) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.

(39) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).

(40) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.

(41) To ensure sustainability and durability of qualified trust services and to boost users’ confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

(42) To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.

(43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body considers that the functioning of a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.

(44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council (9) which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.

(45) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to
facilitating the due diligence leading to the provisioning of qualified trust services.

(46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.

(47) Confidence in and compliance of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly show trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.

(48) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC (10), electronic signatures with a lower security assurance should also be accepted.

(49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.

(50) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

(53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.

(54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

(55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to those for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.

(56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

(57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

(58) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

(59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document’s origin and integrity.

(60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.

(61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

(62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an
advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.

Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.

When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU (11).

In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.

It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.

Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

The concept of ‘legal persons’, according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, ‘legal persons’, within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.

In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission can carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (12).

When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunications Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.

For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.

To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.

Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council (13) and delivered an opinion on 27 September 2012 (14).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:
(a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State; (b) lays down rules for trust services, in particular for electronic transactions; and (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union. 2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants. 3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person; (2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service; (3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established; (4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons; (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed; (6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service; (7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate; (8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15); (9) 'signatory' means a natural person who creates an electronic signature; (10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign; (11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26; (12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures; (13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature; (14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person; (15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I; (16) 'trust service' means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services; (17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation; (18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides; (19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider; (20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body; (21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services; (22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature; (23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II; (24) 'creator of a seal' means a legal person who creates an electronic seal; (25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity; (26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36; (27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal; (28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal; (29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person; (30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III; (31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal; (32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II; (33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
Article 4
Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

Article 5
Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.

2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

CHAPTER II
ELECTRONIC IDENTIFICATION

Article 6
Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;

(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantially or high;

(c) the relevant public sector body uses the assurance level substantially or high in relation to accessing that service online.

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

Article 7
Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

(a) the electronic identification means under the electronic identification scheme are issued:

(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or

(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).
Article 8
Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 9
Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

(b) the applicable supervisory regime and information on the liability regime with respect to the following:

(i) the party issuing the electronic identification means; and

(ii) the party operating the authentication procedure;

(c) the authority or authorities responsible for the electronic identification scheme;

(d) information on the entity or entities which manage the registration of the unique person identification data;

(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

(f) a description of the authentication referred to in point (f) of Article 7;

(g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereof.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2.

The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State’s request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10
Security breach

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11
Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently by any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently by any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently by any natural or legal person due to a failure to ensure the correct
operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.
4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.
5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 12
Cooperation and interoperability

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.
2. For the purposes of paragraph 1, an interoperability framework shall be established.
3. The interoperability framework shall meet the following criteria:
   (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;
   (b) it follows European and international standards, where possible;
   (c) it facilitates the implementation of the principle of privacy by design; and
   (d) it ensures that personal data is processed in accordance with Directive 95/46/EC.
4. The interoperability framework shall consist of:
   (a) a reference to minimum technical requirements related to the assurance levels under Article 8;
   (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
   (c) a reference to minimum technical requirements for interoperability;
   (d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
   (e) rules of procedure;
   (f) arrangements for dispute resolution; and
   (g) common operational security standards.
5. Member States shall cooperate with regard to the following:
   (a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and
   (b) the security of the electronic identification schemes.
6. The cooperation between Member States shall consist of:
   (a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;
   (b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;
   (c) peer review of electronic identification schemes falling under this Regulation; and
   (d) examination of relevant developments in the electronic identification sector.
7. By 19 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.
8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.
9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER III
TRUST SERVICES

SECTION 1
General provisions

Article 13
Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14
International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country or an international organisation in accordance with Article 218 TFEU.

2. Agreements referred to in paragraph 1 shall ensure, in particular, that:
   (a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;
   (b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

Article 15
Accessibility for persons with disabilities

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Article 16
Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

SECTION 2
Supervision

Article 17
Supervisory body

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

3. The role of the supervisory body shall be the following:
   (a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;
   (b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:
   (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;
   (b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);
   (c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);
   (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;
   (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);
   (f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;
   (g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;
   (h) to inform the body responsible for the national trusted service has been provided, the trust service provider of any breach of security or loss of integrity that has a significant impact on the trust service they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

5. Member States may require the supervisory body to perform on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year’s main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).

7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.

8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 18
Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchanging good practice.

A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:
   (a) the supervisory body is not competent to provide the requested assistance;
   (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;
   (c) providing the requested assistance would be incompatible with this Regulation.

3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States’ supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

Article 19
Security requirements applicable to trust service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay. Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts:
   (a) further specify the measures referred to in paragraph 1; and
SECTION 3
Qualified trust services

Article 20
Supervision of qualified trust service providers
1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfill the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.
2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfill the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.
3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfill requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration, and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.
4. The Commission may, by means of implementing acts, establish reference number of the following standards:
   (a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;
   (b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 21
Initiation of a qualified trust service
1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.
2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.
If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.
3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).
4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 22
Trusted lists
1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.
2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.
3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.
4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.
5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 23
EU trust mark for qualified trust services
1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.
2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.
3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24
Requirements for qualified trust service providers
1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and,
The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

(a) by the physical presence of the natural person or of an authorised representative of the legal person; or

(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’; or

(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

(d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

A qualified trust service provider providing qualified trust services shall:

(a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;

(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;

(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

(d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

(f) use trustworthy systems to store data provided to it, in a verifiable form so that:

(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity;

(g) take appropriate measures against forgery and theft of data;

(h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;

(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced
electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28
Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29
Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 30
Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The Commission may, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31
Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32
Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signature in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the electronic signature was created by a qualified electronic signature creation device;

(g) the integrity of the signed data has not been compromised;

(h) the requirements provided for in Article 26 were met at the time of signing.
2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

---

**Article 33**

**Qualified validation service for qualified electronic signatures**

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

   (a) provides validation in compliance with Article 32(1); and

   (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

---

**Article 34**

**Qualified preservation service for qualified electronic signatures**

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

---

**SECTION 5**

**Electronic seals**

**Article 35**

**Legal effects of electronic seals**

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

---

**Article 36**

**Requirements for advanced electronic seals**

An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

---

**Article 37**

**Electronic seals in public services**

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not require for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

---

**Article 38**

**Qualified certificates for electronic seals**

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.

2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.

3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.

4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:

   (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;

   (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be
visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 39
Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.
3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

Article 40
Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

SECTION 6
Electronic time stamps

Article 41
Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42
Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:
   (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
   (b) it is based on an accurate time source linked to Coordinated Universal Time; and
   (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7
Electronic registered delivery services

Article 43
Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44
Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:
   (a) they are provided by one or more qualified trust service provider(s);
   (b) they ensure with a high level of confidence the identification of the sender;
   (c) they ensure the identification of the addressee before the delivery of the data;
   (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
   (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
   (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
2. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.
3. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 8
Website authentication

Article 45
Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER IV
ELECTRONIC DOCUMENTS

Article 46
Legal effects of electronic documents
An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER V
DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.
3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or, if before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 48
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VI
FINAL PROVISIONS

Article 49
Review

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (j) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

Article 50
Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.
2. References to the repealed Directive shall be construed as references to this Regulation.

Article 51
Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.
2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.
3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.
4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

Article 52
Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from 1 July 2016, except for the following:

(a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 23(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;
(b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8); (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).
3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.
4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 23 July 2014.

For the Parliament
The President
M. SCHULZ
For the Council
S. GOZI

(1) OJ C 351, 15.11.2012, p. 73.

ANNEX I
REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
— for a legal person: the name and, where applicable, registration number as stated in the official records,
— for a natural person: the person’s name;
(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
(d) electronic signature validation data that corresponds to the electronic signature creation data;
(e) details of the beginning and end of the certificate’s period of validity;
(f) the certificate identity code, which must be unique for the qualified trust service provider;
(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;
(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II
REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
(b) the electronic signature creation data used for electronic signature creation can practically occur only once;
(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
(a) the security of the duplicated datasets must be at the same level as for the original datasets;
(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

ANNEX III
REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates...
including at least the Member State in which that provider is established and:
— for a legal person: the name and, where applicable, registration number as stated in the official records,
— for a natural person: the person’s name;
(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;
(d) electronic seal validation data, which corresponds to the electronic seal creation data;
(e) details of the beginning and end of the certificate’s period of validity;
(f) the certificate identity code, which must be unique for the qualified trust service provider;
(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
(i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;
(j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX IV
REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
— for a legal person: the name and, where applicable, registration number as stated in the official records,
— for a natural person: the person’s name;
(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;
for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;
(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;
(f) details of the beginning and end of the certificate’s period of validity;
(g) the certificate identity code, which must be unique for the qualified trust service provider;
(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;
(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.
Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14

Article 5 – Right to liberty and security

1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:
   a. the lawful detention of a person after conviction by a competent court;
   b. the lawful arrest or detention of a person for non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;
   c. the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;
   d. the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;
   e. the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;
   f. the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.

2. Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him.

3. Everyone arrested or detained in accordance with the provisions of paragraph 1c of this article shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial.

4. Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.

5. Everyone who has been the victim of arrest or detention in contravention of the provisions of this article shall have an enforceable right to compensation.

Article 6 – Right to a fair trial

6. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

7. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

8. Everyone charged with a criminal offence has the following minimum rights:
   a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
   b. to have adequate time and facilities for the preparation of his defence;
   c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
   d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
   e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except well-being of the country, for the prevention of disorder or crime, for the protection of health or...
Article 9 – Freedom of thought, conscience and religion

1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.

2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.

Article 10 – Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[...]

Article 13 – Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.
Charter of Fundamental Rights of the European Union
(2007/C 303/01)

[...]
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data


Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I – General provisions

Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 – Definitions

For the purposes of this convention:

"personal data" means any information relating to an identified or identifiable individual ("data subject");

"automated data file" means any set of data undergoing automatic processing;

"automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

"controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 – Scope

The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law.

Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Chapter II – Basic principles for data protection

Article 4 – Duties of the Parties

Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

obtained and processed fairly and lawfully;

stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

adequate, relevant and not excessive in relation to the purposes for which they are stored;

accurate and, where necessary, kept up to date;

preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
Article 6 – Special categories of data
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 – Data security
Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 – Additional safeguards for the data subject
Any person shall be enabled:
to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 – Exceptions and restrictions
No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
protecting the data subject or the rights and freedoms of others.

Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 – Sanctions and remedies
Each Party shall undertake to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 – Extended protection
None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

Chapter III – Transborder data flows

Article 12 – Transborder flows of personal data and domestic law
The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties
The Parties agree to render each other mutual assistance in order to implement this convention.

For that purpose:
each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
each Party which has designated more than one authority shall specify in its communication referred to in the previous subparagraph the competence of each authority.

An authority designated by a Party shall at the request of an authority designated by another Party:
furnish information on its law and administrative practice in the field of data protection;
take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 – Assistance to data subjects resident abroad
Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

When such a person resides in the territory of another Party, he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

The request for assistance shall contain all the necessary particulars, relating inter alia to:
the name, address and any other relevant particulars identifying the person making the request;
the automated personal data file to which the request pertains, or its controller;
the purpose of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities
An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information
for purposes other than those specified in the request for assistance.

Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 – Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

- the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;
- the request does not comply with the provisions of this convention;
- compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 – Costs and procedures of assistance

Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter V – Consultative Committee

Article 18 – Composition of the committee

A Consultative Committee shall be set up after the entry into force of this convention.

Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19 – Functions of the committee

The Consultative Committee:

- may make proposals with a view to facilitating or improving the application of the convention;
- may make proposals for amendment of this convention in accordance with Article 21;
- shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;
- may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20 – Procedure

The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

Chapter VI – Amendments

Article 21 – Amendments

Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Chapter VII – Final clauses

Article 22 – Entry into force

This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-member States

After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for
in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

**Article 24 – Territorial clause**

Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

**Article 25 – Reservations**

No reservation may be made in respect of the provisions of this convention.

**Article 26 – Denunciation**

Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

**Article 27 – Notifications**

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

- any signature;
- the deposit of any instrument of ratification, acceptance, approval or accession;
- any date of entry into force of this convention in accordance with Articles 22, 23 and 24;
- any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

---

**Relevant Case-Law on Convention for the Protection of Human Rights and Fundamental Freedoms**

**CASE OF KASS AND OTHERS v. GERMANY**  
(Application no. 5029/71)

**JUDGMENT**

STRASBOURG  
6 September 1978

[...]

**PROCEDURE**

1. The case of Klass and others was referred to the Court by the European Commission of Human Rights (hereinafter called “the Commission”). The case originated in an application against the Federal Republic of Germany lodged with the Commission on 11 June 1971 under Article 25 (art. 25) of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter called “the Convention”) by five German citizens, namely Gerhard Klass, Peter Lubberger, Jürgen Nussbruch, Hans-Jürgen Pohl and Dieter Selb.

[...]

**AS TO THE FACTS**

10. The applicants, who are German nationals, are Gerhard Klass, an Oberstaatsanwalt, Peter Lubberger, a lawyer, Jürgen Nussbruch, a judge, Hans-Jürgen Pohl and Dieter Selb, lawyers. Mr. Nussbruch lives in Heidelberg, the others in Mannheim.

All five applicants claim that Article 10 para. 2 of the Basic Law (Grundgesetz) and a statute enacted in pursuance of that provision, namely the Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, hereinafter referred to as “the G 10”), are contrary to the Convention. They do not dispute that the State has the right to have recourse to the surveillance measures contemplated by the legislation; they challenge this legislation in that it permits those measures without obliging the authorities in every case to notify the persons concerned after the event, and in that it excludes any remedy before the courts against the ordering and execution of such measures. Their application is directed against the legislation as modified and interpreted by the Federal Constitutional Court (Bundesverfassungsgericht).

11. Before lodging their application with the Commission, the applicants had in fact appealed to the Federal Constitutional Court. By judgment of 15 December 1970, that Court held that Article 1 para. 5, sub-paragraph 5 of the G 10 was void, being incompatible with the second sentence of Article 10 para. 2 of the Basic Law, in so far as it excluded notification of the person concerned about the measures of surveillance even when such notification could be given without jeopardising the purpose of the restriction. The Constitutional Court dismissed the remaining claims (Collected Decisions of the Constitutional Court, Vol. 30, pp. 1 et seq.). Since the operative provisions of the aforementioned judgment have the force of law, the competent authorities are bound to apply the G 10 in the form and subject to the
interpretation decided by the Constitutional Court. Furthermore, the Government of the Federal Republic of Germany were prompted by this judgment to propose amendments to the G 10, but the parliamentary proceedings have not yet been completed.

12. As regards the applicants’ right to apply to the Constitutional Court, that Court held, inter alia: “In order to be able to enter a constitutional application against an Act, the applicant must claim that the Act itself, and not merely an implementary measure, constitutes a direct and immediate violation of one of his fundamental rights … These conditions are not fulfilled since, according to the applicants’ own submissions, it is only by an act on the part of the executive that their fundamental rights would be violated. However, because they are not appraised of the interference with their rights, the persons concerned cannot challenge any implementary measure. In such cases, they must be entitled to make a constitutional application against the Act itself, as in cases where a constitutional application against an implementary measure is impossible for other reasons …” (ibid, pp. 16-17).

13. Although, as a precautionary measure, the applicants claimed before both the Constitutional Court and the Commission that they were being subjected to surveillance measures, they did not know whether the G 10 had actually been applied to them. On this point, the Agent of the Government made the following declaration before the Court: “To remove all uncertainty as to the facts of the case and to give the Court a clear basis for its decision, the Federal Minister of the Interior, who has competence in the matter, has, with the G 10’s Commission’s approval, authorised me to make the following statement: At no time have surveillance measures provided for by the Act enacted in pursuance of Article 10 of the Basic Law been ordered or implemented against the applicants. Neither as persons suspected of one or more of the offences specified in the Act nor as third parties within the meaning of Article 1, paragraph 2, sub-paragraph 2, of the G 10 have the applicants been subjected to such measures. There is also no question of the applicants’ having been indirectly involved in a surveillance measure directed against another person - at least, not in any fashion which would have permitted their identification. Finally, there is no question of the applicants’ having been subjected to surveillance by mistake - for example through confusion over a telephone number -, since in such cases the person concerned is notified of the surveillance measure.”

The contested legislation

14. After the end of the Second World War, the surveillance of mail, post and telecommunications in Germany was dealt with by the occupying powers. As regards the Federal Republic, neither the entry into force on 24 May 1949 of the Basic Law nor the foundation of the State of the Federal Republic on 20 September 1949 altered this situation which continued even after the termination of the occupation régime in 1955. Article 5 para. 2 of the Convention of 26 May 1952 on Relations between the Three Powers (France, the United States and the United Kingdom) and the Federal Republic - as amended by the Paris Protocol of 23 October 1954 - specified in fact that the Three Powers temporarily retained “the rights … heretofore held or exercised by them, which relate to the protection of the security of armed forces stationed in the Federal Republic”. Under the same provision, these rights were to lapse “when the appropriate German authorities [had] obtained similar powers under German legislation enabling them to take effective action to protect the security of those forces, including the ability to deal with a serious disturbance of public security and order”. 15. The Government wished to substitute the domestic law for the rights exercised by the Three Powers and to place under legal control interferences with the right, guaranteed by Article 10 of the Basic Law, to respect for correspondence. Furthermore, the restrictions to which this right could be subject appeared to the Government to be inadequate for the effective protection of the constitutional order of the State. Thus, on 13 June 1967, the Government introduced two Bills as part of the Emergency Legislation. The first sought primarily to amend Article 10 para. 2 of the Basic Law; the second - based on Article 10 para. 2 so amended - was designed to limit the right to secrecy of the mail, post and telecommunications. The two Acts, having been adopted by the federal legislative assemblies, were enacted on 24 June and 13 August 1968 respectively.

The Three Powers had come to the view on 27 May that these two texts met the requirements of Article 5 para. 2 of the above-mentioned Convention. Their statements declared: “The rights of the Three Powers heretofore held or exercised by them which relate to the protection of the security of armed forces stationed in the Federal Republic and which are temporarily retained pursuant to that provision will accordingly lapse as each of the above-mentioned texts, as laws, becomes effective.”

16. In its initial version, Article 10 of the Basic Law guaranteed the secrecy of mail, post and telecommunications with a proviso that restrictions could be ordered only pursuant to a statute. As amended by the Act of 24 June 1968, it now provides: “(1) Secrecy of the mail, post and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a statute. Where such restrictions are intended to protect the free democratic constitutional order or the existence or security of the Federation or of a Land, the statute may provide that the person concerned shall not be notified of the restriction and that legal remedy through the courts shall be replaced by a system of scrutiny by agencies and auxiliary agencies appointed by the people’s elected representatives.”

17. The G 10, adopting the solution contemplated by the second sentence of paragraph 2 of the above-quoted Article 10, specifies (in Article 1 para. 1) the cases in which the competent authorities may impose the restrictions provided for in that paragraph, that is to say, may open and inspect mail and post, read telegraphic messages, listen to and record telephone conversations. Thus, Article 1 para. 1 empowers those authorities so to act in order to protect against “imminent dangers” threatening the “free democratic constitutional order”, “the existence or the security of the Federation or of a Land”, “the security of the (allied) armed forces” stationed on the territory of the Republic and the security of “the troops of one of the Three Powers stationed in the Land of Berlin”. According to Article 1 para. 2, these measures may be taken only where there are factual indications (tatsächlichen Anhaltspunkte) for suspecting a person of planning, committing or having committed certain criminal acts punishable under the Criminal Code, such as offences against the peace or security of the State (sub-paragraph 1, no. 1), the democratic order (sub-paragraph 1, no. 2), external security (sub-paragraph 1, no. 3) and the security of the allied armed forces (sub-paragraph 1, no. 5).

Paragraph 2 of Article 1 further states that the surveillance provided for in paragraph 1 is permissible only if the establishment of the facts by another method is without prospects of success or considerably more difficult (aussichtlos oder wesentlich erschwert). The surveillance may cover only “the suspect or such other persons who are, on the basis of clear facts (bestimmt Tatsachen), to be presumed to receive or forward communications intended for the suspect or emanating from him or whose telephone the suspect is to be presumed to use” (sub-paragraph 2).
18. Article 1 para. 4 of the Act provides that an application for surveillance measures may be made only by the head, or his substitute, of one of the following services: the Agencies for the Protection of the Constitution of the Federation and the Länder: the Bundesamt für Verfassungsschutz (Verfassungsschutzbehörden der Länder), the Army Security Office (Amt für Sicherheit der Bundeswehr) and the Federal Intelligence Service (Bundesnachrichtendienst).

The measures are ordered, on written application giving reasons, either by the supreme Land authority in cases falling within its jurisdiction or by a Federal Minister empowered for the purpose by the Chancellor. The Chancellor has entrusted these functions to the Ministers of the Interior and of Defence each of whom, in the sphere falling within his competence, must personally take the decision as to the application of the measures (Article 1 para. 5, sub-paragraphs 1 and 2). Measures ordered must be immediately discontinued once the required conditions have ceased to exist or the measures themselves are no longer necessary (Article 1 para. 7, sub-paragraph 2). The measures remain in force for a maximum of three months and may be renewed only on fresh application (Article 1 para. 5, sub-paragraph 3).

19. Under the terms of Article 1 para. 5, sub-paragraph 5, the person concerned is not to be notified of the restrictions affecting him. However, since the Federal Constitutional Court's judgment of 15 December 1970 (see paragraph 11 above) the competent authority has to inform the person concerned as soon as notification can be made without jeopardising the purpose of the restriction. To this end, the Minister concerned considers ex officio, immediately the measures have been discontinued or, if need be, at regular intervals thereafter, whether the person concerned should be notified. The Minister submits his decision for approval to the Commission set up under the G 10 for the purpose of supervising its application (hereinafter called "the G 10 Commission"). The G 10 Commission may direct the Minister to inform the person concerned that he has been subjected to surveillance measures.

20. Implementation of the measures ordered is supervised by an official qualified for judicial office (Article 1 para. 7, sub-paragraph 1). This official examines the information obtained in order to decide whether its use would be compatible with the Act and whether it is relevant to the purpose of the measure. He transmits to the competent authorities only information satisfying these conditions and destroys any other intelligence that may have been gathered.

The information and documents so obtained may not be used for other ends and documents must be destroyed as soon as they are no longer needed to achieve the required purpose (Article 1 para. 7 sub-paragraphs 3 and 4).

21. The competent Minister must, at least once every six months, report to a Board consisting of five Members of Parliament on the application of the G 10; the Members of Parliament are appointed by the Bundestag in proportion to the parliamentary groupings, the opposition being represented on the Board (Article 1 para. 9, sub-paragraph 1, of the G 10 and Rule 12 of the Rules of Procedure of the Bundestag). In addition, the Minister is bound every month to provide the G 10 Commission with an account of the measures he has ordered (Article 1 para. 9). In practice and except in urgent cases, the Minister seeks the prior consent of this Commission. The Government, moreover, intend proposing to Parliament to amend the G 10 so as to make such prior consent obligatory.

The G 10 Commission decides, ex officio or on application by a person believing himself to be under surveillance, on both the legality of and the necessity for the measures; if it declares any measures to be illegal or unnecessary, the Minister must terminate them immediately (Article 1 para. 9, sub-paragraph 2). Although not required by the Constitutional Court’s judgment of 15 December 1970, the Commission has, since that judgment, also been called upon when decisions are taken on whether the person concerned should be notified of the measures affecting him (see paragraph 19 above).

The G 10 Commission consists of three members, namely, a Chairman, who must be qualified to hold judicial office, and two assessors. The Commission members are appointed for the current term of the Bundestag by the above-mentioned Board of five Members of Parliament after consultation with the Government; they are completely independent in the exercise of their functions and cannot be subject to instructions.

The G 10 Commission draws up its own rules of procedure which must be approved by the Board; before taking this decision, the Board consults the Government.

For the Länder, their legislatures lay down the parliamentary supervision to which the supreme authorities are subject in the matter. In fact, the Länder Parliaments have set up supervisory bodies which correspond to the federal bodies from the point of view of organisation and operation.

22. According to Article 1 para. 9, sub-paragraph 5, of the G 10: “... there shall be no legal remedy before the courts in respect of the ordering and implementation of restrictive measures.”

The official statement of reasons accompanying the Bill contains the following passage in this connection: "The surveillance of the post and telecommunications of a person who is under surveillance may serve a useful purpose only if the person concerned does not become aware of it. For this reason, notification to this person is out of the question. For the same reason, it must be avoided that a person who intends to commit, or who has committed, the offences enumerated in the Act can, by using a legal remedy, inform himself whether he is under surveillance. Consequently, a legal remedy to impugn the ordering of restrictive measures had to be denied..."

The Bill presented during the 4th legislative session... provided for the ordering (of such measures) by an independent judge. The Federal Government abandoned this solution in the Bill amending Article 10 of the Basic Law, introduced as part of the Emergency Legislation, mainly because the Executive, which is responsible before the Bundestag, should retain the responsibility for such decisions in order to observe a clear separation of powers. The present Bill therefore grants the power of decision to a Federal Minister or the supreme authority of the Land... mentioned reasons — the person concerned is deprived of the opportunity of having the restrictive measures ordered examined by a court; on the other hand, the constitutional principle of government under the rule of law demands an independent control of interference by the Executive with the rights of citizens. Thus, the Bill, in pursuance of the Bill amending Article 10 of the Basic Law..., prescribes the regular reporting to a Parliamentary Board and the supervision of the ordering of the restrictive measures by a Control Commission appointed by the Board..." (Bundestag document V/1880 of 13 June 1967, p. 8).

23. Although access to the courts to challenge the ordering and implementation of surveillance measures is excluded in this way, it is still open to a person believing himself to be under surveillance pursuant to the G 10 to seek a constitutional remedy; according to the information supplied by the Government, a person who has applied to the G 10 Commission without success retains the right to apply to the Constitutional Court. The latter may reject the application on the ground that the applicant is unable to adduce proof to substantiate a complaint, but it may also request the Government concerned to supply it with information or to produce documents to enable it to verify for itself the individual’s allegations. The authorities are bound to reply to such a request even if the information asked for is secret. It is then for the Constitutional Court to decide whether the information and documents so obtained can be used; it may decide by a two-thirds majority that their use is incompatible...
with State security and dismiss the application on that ground (Article 26 para. 2 of the Constitutional Court Act).

The Agent of the Government admitted that this remedy might be employed only on rare occasions.

24. If the person concerned is notified, after the measures have been discontinued, that he has been subject to surveillance, several legal remedies against the interference with his rights become available to him. According to the information supplied by the Government, the individual may: in an action for a declaration, have reviewed by an administrative court declaration, the legality of the application to him of the G 10 and the conformity with the law of the surveillance measures ordered; bring an action for damages in a civil court if he has been prejudiced; bring an action for the destruction or, if appropriate, restitution of documents; finally, if none of these remedies is successful, apply to the Federal Constitutional Court for a ruling as to whether there has been a breach of the Basic Law.

25. Article 2 of the G 10 has also amended the Code of Criminal Procedure by inserting therein two Articles which authorise measures of surveillance of telephone and telegraphic communications.

Under Article 100 (a), these measures may be taken under certain conditions, in particular, when there are clear facts on which to suspect someone of having committed or attempted to commit certain serious offences listed in that Article. Under Article 100 (b), such measures may be ordered only by a court and for a maximum of three months; they may be renewed. In urgent cases, the decision may be taken by the public prosecutor’s department but to remain in effect it must be confirmed by a court within three days. The persons concerned and informed of the measures taken in their respect as soon as notification can be made without jeopardising the purpose of the investigation (Article 101 para. 1 of the Code of Criminal Procedure).

These provisions are not, however, in issue in the present case.

[...]

AS TO THE LAW

I. ON ARTICLE 25 PARA. 1 (art. 25-1)

30. Both in their written memorial and in their oral submissions, the Government formally invited the Court to find that the application lodged with the Commission was "inadmissible". They argued that the applicants could not be considered as "victims" within the meaning of Article 25 para. 1 (art. 25-1) which provides as follows:

"The Commission may receive petitions addressed to the Secretary-General of the Council of Europe from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in this Convention, provided that the High Contracting Party against which the complaint has been lodged has declared that it recognises the competence of the Commission to receive such petitions ..."

In the Government’s submission, the applicants were not claiming to have established an individual violation, even potential, of their own rights but rather, on the basis of the purely hypothetical possibility of being subject to surveillance, were seeking a general and abstract review of the contested legislation in the light of the Convention.

31. According to the reply given by the Delegates at the hearing, the Commission agreed with the Government that the Court is competent to determine whether the applicants can claim to be “victims” within the meaning of Article 25 para. 1 (art. 25-1). However, the Commission disagreed with the Government in so far as the latter’s proposal might imply the suggestion that the Commission’s decision on the admissibility of the application should as such be reviewed by the Court.

The Delegates considered that the Government were requiring too rigid a standard for the notion of a “victim” of an alleged breach of Article 8 (art. 8) of the Convention. They submitted that, in order to be able to claim to be the victim of an interference with the exercise of the right conferred on him by Article 8 para. 1 (art. 8-1), it should suffice that a person is in a situation where there is a reasonable risk of his being subjected to secret surveillance. In the Delegates’ view, the applicants are not to be considered as constructive victims, as the Commission had in effect stated: they can claim to be direct victims of a violation of their rights under Article 8 (art. 8) in that under the terms of the contested legislation everyone in the Federal Republic of Germany who could be presumed to have contact with people involved in subversive activity really runs the risk of being subject to secret surveillance, the sole existence of this risk being in itself a restriction on free communication.

The Principal Delegate, for another reason, regarded the application as rightly declared admissible. In his view, the alleged violation related to a single right which, although not expressly enunciated in the Convention, was to be derived by necessary implication; this implied right was the right of every individual to be informed within a reasonable time of any secret measure taken in his respect by the public authorities and amounting to an interference with his rights and freedoms under the Convention.

32. The Court confirms the well-established principle of its own case-law that, once a case is duly referred to it, the Court is endowed with full jurisdiction and may take cognisance of all questions of fact or of law arising in the course of the proceedings, including questions which may have been raised before the Commission under the head of admissibility. This conclusion is in no way invalidated by the powers conferred on the Commission under Article 27 (art. 27) of the Convention as regards the admissibility of applications. The task which this Article assigns to the Commission is one of sifting; the Commission either does or does not accept the applications. Its decision to reject applications which it considers to be inadmissible are without appeal as are, moreover, also those by which applications are accepted; they are taken in complete independence (see the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 29 and 30, paras. 47-54; see also the judgment of 9 February 1967 on the preliminary objection in the "Belgian Linguistic" case, Series A no. 5, p. 18; the Handyside judgment of 7 December 1976, Series A no. 24, p. 20, para. 41; and the judgment of 18 January 1978 in the case of Ireland v. the United Kingdom, Series A no. 25, p. 63, para. 157).

The present case concerns, inter alia, the interpretation of the notion of "victim" within the meaning of Article 25 (art. 25) of the Convention, this being a matter already raised before the Commission. The Court therefore affirms its jurisdiction to examine the issue arising under that Article (art. 25).

33. While Article 24 (art. 24) allows each Contracting State to refer to the Commission any alleged breach of the Convention by another Contracting State, a person, non-governmental organisation or group of individuals must, in order to be able to lodge a petition in pursuance of Article 25 (art. 25), claim "to be the victim of a violation ... of the rights set forth in (the) Convention". Thus, in contrast to the position under Article 24 (art. 24) - where, subject to the other conditions laid down, the general interest attaching to the observance of the Convention renders admissible an inter-State application - Article 25 (art. 25) requires that an individual applicant should claim to have been actually affected by the violation he alleges (see the judgment of 18 January 1978 in the case of Ireland v. the United Kingdom, Series A no. 25, pp. 90-91, paras. 239 and 240). Article 25 (art. 25) does not institute for individuals a kind of actio popularis for the interpretation of the Convention; it does not permit
individuals to complain against a law in abstracto simply because they feel that it contravenes the Convention. In principle, it does not suffice for an individual applicant to claim that the mere existence of a law violates his rights under the Convention; it is necessary that the law should have been applied to his detriment. Nevertheless, as both the Government and the Commission pointed out, a law may by itself violate the rights of an individual if the individual is directly affected by the law in the absence of any specific measure of implementation. In this connection, the Court recalls that in two previous cases dealing with applications lodged in pursuance of Article 25 (art. 25), it has itself been faced with legislation having such an effect: in the "Belgian Linguistic" case and the case of Kjeldsen, Busk Madsen and Pedersen, the Court was called on to examine the compatibility with the Convention and Protocol No. 1 of certain legislation relating to education (see the judgment of 23 July 1968, Series A no. 6, and the judgment of 7 December 1976, Series A no. 23, especially pp. 22-23, para. 48).

34. Article 25 (art. 25), which governs the access by individuals to the Commission, is one of the keystones in the machinery for the enforcement of the rights and freedoms set forth in the Convention. This machinery involves, for an individual who considers himself to have been prejudiced by some action claimed to be in breach of the Convention, the possibility of bringing the alleged violation before the Commission, which provided the other admissibility requirements are satisfied. The question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious.

The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occurring by the mere existence of a secret measure or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.

35. In the light of these considerations, it has now to be ascertained whether, by reason of the particular legislation being challenged, the applicants can claim to be victims, in the sense of Article 25 (art. 25), of a violation of Article 8 (art. 8) of the Convention - Article 8 (art. 8) being the provision giving rise to the central issue in the present case.

36. The Court points out that where a State institutes secret surveillance, the existence of what is unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 (art. 8), or even to be deprived of the right granted by that Article (art. 8) without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions. In this connection, it should be recalled that the Federal Constitutional Court in its judgment of 15 December 1970 (see paragraphs 11 and 12 above) adopted the following reasoning:

"In order to be able to enter a constitutional application against an Act, the applicant must claim that the Act itself, and not merely an implementary measure, constitutes a direct and immediate violation of one of his fundamental rights ... These conditions are not fulfilled since, according to the applicants' own submissions, it is only by an act on the part of the executive that their fundamental rights would be violated. However, because they are not apprised of the interference with their rights, the persons concerned cannot challenge any implementary measure. In such cases, they must be entitled to make a constitutional application against the Act itself, as in such cases where a constitutional application against an implementary measure is impossible for other reasons ..."

This reasoning, in spite of the possible differences existing between appeals to the Federal Constitutional Court under German law and the enforcement machinery set up by the Convention, is valid mutatis mutandis, for applications lodged under Article 25 (art. 25).

The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 (art. 25), since otherwise Article 8 (art. 8) runs the risk of being nullified.

37. As to the facts of the particular case, the Court observes that the contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing that the legislation has been either some indiscretion or subsequent notification in the circumstances laid down in the Federal Constitutional Court's judgment (see paragraph 11 above). To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore, as the Delegates rightly pointed out, this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 (art. 8).

At the hearing, the Agent of the Government informed the Court that at no time had the measures or part thereof been ordered or implemented in respect of the applicants (see paragraph 13 above). The Court takes note of the Agent's statement. However, in the light of its conclusions as to the effect of the contested legislation the Court does not consider that this retrospective clarification bears on the appreciation of the applicants' status as victims.

38. Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to "[claim to be the victim of a violation" of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions.

Accordingly, the Court does not find it necessary to decide whether the Convention implies a right to be informed in the circumstances mentioned by the Principal Delegate.

II. ON THE ALLEGED VIOLATION OF ARTICLE 8 (art. 8)

39. The applicants claim that the contested legislation, notably because the person concerned is not informed of the surveillance measures and cannot have recourse to the courts when such measures are terminated, violates Article 8 (art. 8) of the Convention which provides as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence."
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

40. According to Article 10 para. 2 of the Basic Law, restrictions upon the secrecy of the mail, post and telecommunications may be ordered but only pursuant to a statute. Article 1 para. 1 of the G 10 allows certain authorities to open and inspect mail and post, to read telegraphic messages and to monitor and record telephone conversations (see paragraph 17 above). The Court's examination under Article 8 (art. 8) is thus limited to the authorisation of such measures alone and does not extend, for instance, to the secret surveillance effect in pursuance of the Code of Criminal Procedure (see paragraph 25 above).

41. The first matter to be decided is whether and, if so, in what respect the contested legislation, in permitting the above-mentioned measures of surveillance, constitutes an interference with the exercise of the right guaranteed to the applicants under Article 8 para. 1 (art. 8-1).

Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision.

In its report, the Commission expressed the opinion that the secret surveillance provided for under the German legislation amounted to an interference with the exercise of the right set forth in Article 8 para. 1 (art. 8-1). Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference with a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the secret surveillance legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and correspondence.

The Court does not exclude that the contested legislation, and therefore the measures permitted thereunder, could also involve an interference with the exercise of a person's right to respect for his home. However, the Court does not deem it necessary in the present proceedings to decide this point.

42. The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.

43. In order for the "interference" established above not to infringe Article 8 (art. 8), it must, according to paragraph 2 (art. 8-2), first of all have been "in accordance with the law". This requirement is fulfilled in the present case since the "interference" results from Acts passed by Parliament, including one Act which was modified by the Federal Constitutional Court, in the exercise of its jurisdiction, by its judgment of 15 December 1970 (see paragraph 11 above). In addition, the Court observes that, as both the Government and the Commission pointed out, any individual measure of surveillance has to comply with the strict conditions and procedures laid down in the legislation itself.

44. It remains to be determined whether the other requisites laid down in paragraph 2 of Article 8 (art. 8-2) were also satisfied. According to the Government and the Commission, the interference permitted by the contested legislation was "necessary in a democratic society in the interests of national security" and/or "for the prevention of disorder or crime".

Before the Court the Government submitted that the interference was additionally justified "in the interests of public safety" and "for the protection of the rights and freedoms of others".

45. The G 10 defines precisely, and thereby limits, the purposes for which the restrictive measures may be imposed. It provides that, in order to protect against "imminent dangers" threatening "the free democratic constitutional order", "the existence or security of the Federation or of a Land", "the security of the (allied) armed forces" stationed on the territory of the Republic or the security of "the troops of one of the Three Powers stationed on the Land of Berlin", the responsible authorities may authorise the restrictions referred to above (see paragraph 17).

46. The Court, sharing the view of the Government and the Commission, finds that the aim of the G 10 is indeed to safeguard national security and/or to prevent disorder or crime in pursuance of Article 8 para. 2 (art. 8-2). In these circumstances, the Court does not deem it necessary to decide whether the further purposes cited by the Government are also relevant.

On the other hand, it has to be ascertained whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society.

47. The applicants do not object to the German legislation in that it provides for wide-ranging powers of surveillance; they accept such powers, and the resultant encroachment upon the right guaranteed by Article 8 para. 1 (art. 8-1), as being a necessary means of defence for the protection of the democratic State. The applicants consider, however, that paragraph 2 of Article 8 (art. 8-2) lays down for such powers certain limits which have to be respected in a democratic society in order to ensure that the society does not slide imperceptibly towards totalitarianism. In their view, the contested legislation lacks adequate safeguards against possible abuse.

48. As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (cf., mutatis mutandis, the De
Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 45-46, para. 93, and the Golder judgment of 21 February 1975, Series A no. 18, pp. 21-22, para. 45; cf., for Article 10 para. 2, the Engel and others judgment of 8 June 1976, Series A no. 22, pp. 41-42, para. 100, and the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, para. 449). Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the grounds of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

50. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law. The functioning of the system of secret surveillance established by the contested legislation, as modified by the Federal Constitutional Court's judgment of 15 December 1970, must therefore be examined in the light of the Convention.

51. According to the G 10, a series of limitative conditions have to be satisfied before a surveillance measure can be imposed. Thus, the permissible restrictive measures are confined to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contact-persons" (see paragraph 17 above). Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation. Surveillance may be ordered only on written application giving reasons, and such an application may be made only by the head, or his substitute, of certain services; the decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor, where appropriate, by the supreme Land authority (see paragraph 18 above). Accordingly, under the law there exists an administrative procedure designed to ensure that measures are not ordered haphazardly, irregularly or without due and proper consideration. In addition, although not required by the Act, the competent Minister must, at least once every six months, report on the application of the G 10 to the Parliamentary Board consisting of five Members of Parliament; the Members of Parliament are appointed by the Bundestag in proportion to the parliamentary groupings, the opposition being represented on the Board. In addition, the Minister is bound every month to provide the G 10 Commission with an account of the measures he has ordered. In practice, he seeks the prior consent of this Commission. The latter decides, ex officio or on application by a person believing himself to be under surveillance, on both the legality and the necessity for the measures in question; if it declares any measures to be illegal or unnecessary, the Minister must terminate them immediately. The Commission members are appointed for the current term of the Bundestag by the Parliamentary Board after consultation with the Government; they are completely independent in the exercise of their functions and cannot be subject to instructions (see paragraph 21 above).

52. The G 10 also lays down strict conditions with regard to the implementation of the surveillance measures and to the processing of the information thereby obtained. The measures in question remain in force for a maximum of three months and may be renewed only on fresh application; the measures must immediately be discontinued once the required conditions have ceased to exist or the measures themselves are no longer necessary: knowledge and documents thereby obtained may not be used for other ends, and documents must be destroyed as soon as they are no longer needed to achieve the required purpose (see paragraphs 18 and 20 above). As regards the implementation of the measures, an initial control is carried out by an official qualified for judicial office. This official examines the information obtained before transmitting to the competent services such information as may be used in accordance with the Act and is relevant to the purpose of the measure; he destroys any other intelligence that may have been gathered (see paragraph 20 above).

53. Under the G 10, while recourse to the courts in respect of the ordering and implementation of measures of surveillance is excluded, subsequent control or review is provided instead, in accordance with Article 10 para. 2 of the Basic Law, by two bodies appointed by the people's elected representatives, namely, the Parliamentary Board and the G 10 Commission. The competent Minister must, at least once every six months, report on the application of the G 10 to the Parliamentary Board consisting of five Members of Parliament; the Members of Parliament are appointed by the Bundestag in proportion to the parliamentary groupings, the opposition being represented on the Board. In addition, the Minister is bound every month to provide the G 10 Commission with an account of the measures he has ordered. In practice, he seeks the prior consent of this Commission. The latter decides, ex officio or on application by a person believing himself to be under surveillance, on both the legality and the necessity for the measures in question; if it declares any measures to be illegal or unnecessary, the Minister must terminate them immediately. The Commission members are appointed for the current term of the Bundestag by the Parliamentary Board after consultation with the Government; they are completely independent in the exercise of their functions and cannot be subject to instructions (see paragraph 21 above).

54. The Government maintain that Article 8 para. 2 (art. 8-2) does not require judicial control of secret surveillance and that the system of review established under the G 10 does effectively protect the rights of the individual. The applicants, on the other hand, qualify this system as a "form of political control", inadequate in comparison with the principle of judicial control which ought to prevail. It therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" resulting from the contested legislation to what is "necessary in a democratic society".

55. Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individuals' rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention (see the Golder judgment of 21 February 1975, Series A no. 18, pp. 16-17, para. 34). The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort; judicial control offering the best guarantees of independence, impartiality and a proper procedure.

56. Within the system of surveillance established by the G 10, judicial control was excluded, being replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.
Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling.

The Court notes in addition that an individual believing himself to be under surveillance has the opportunity of complaining to the G 10 Commission and of having recourse to the Constitutional Court (see paragraph 23 above). However, as the Government conceded, these are remedies which can come into play only in exceptional circumstances.

57. As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual’s participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality.

The applicants’ main complaint under Article 8 (art. 8) is in fact that the person concerned is not always subsequently informed after the suspension of surveillance and is not therefore in a position to seek an effective remedy before the courts. Their preoccupation is the danger of measures being improperly implemented without the individual knowing or being able to verify the extent to which his rights have been interfered with. In their view, effective control by the courts after the suspension of surveillance measures is necessary in a democratic society to ensure against abuses; otherwise adequate control of secret surveillance is lacking and the right conferred on individuals under Article 8 (art. 8) is simply eliminated.

In the Government’s view, the subsequent notification which must be given since the Federal Constitutional Court’s judgment (see paragraphs 11 and 19 above) corresponds to the requirements of Article 8 para. 2 (art. 8-2). In their submission, the whole efficacy of secret surveillance requires that notification be given and after the event cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted. They stressed that recourse to the courts is no longer excluded after notification has been given, various legal remedies then becoming available to allow the individual, inter alia, to seek redress for any injury suffered (see paragraph 24 above).

58. In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.

The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court’s view, in so far as the ‘interference’ resulting from the contested legislation is in principle justified under Article 8 para. 2 (art. 8-2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the ‘interference’. Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court’s judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above).

59. Both in general and in relation to the question of subsequent notification, the applicants have constantly invoked the danger of abuse as a ground for their contention that the legislation they challenge does not fulfil the requirements of Article 8 para. 2 (art. 8-2) of the Convention. While the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the considerations that matter for the purposes of the Court’s present review are the likelihood of such action and the safeguards provided to protect against it.

The Court has examined above (at paragraphs 51 to 58) the contested legislation in the light, inter alia, of these considerations. The Court notes in particular that the G 10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue.

The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention (see, mutatis mutandis, the judgment of 23 July 1968 in the “Belgian Linguistic” case, Series A no. 6, p. 32, para. 5). As the Preamble to the Convention states, “Fundamental Freedoms ... are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend”. In the context of Article 8 (art. 8), this means that a balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole.

60. In the light of these considerations and of the detailed examination of the contested legislation, the Court concludes that before and after the event the information cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted. They stressed that recourse to the courts is no longer excluded after notification has been given, various legal remedies then becoming available to allow the individual, inter alia, to seek redress for any injury suffered (see paragraph 24 above).

III. ON THE ALLEGED VIOLATION OF ARTICLE 13 (art. 13)

61. The applicants also alleged a breach of Article 13 (art. 13) which provides: “Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.”

62. In the applicants’ view, the Contracting States are obliged under Article 13 (art. 13) to provide an effective remedy for any alleged breach of the Convention; any other interpretation of this provision would render it meaningless. On the other hand, both the Government and the Commission consider that there is no basis for the application of Article 13 (art. 13).
63. In the judgment of 6 February 1976 in the Swedish Engine Drivers' Union case, the Court, having found there to be in fact an effective remedy before a national authority, considered that it was not called upon to rule whether Article 13 (art. 13) was applicable only when a right guaranteed by another Article of the Convention has been violated (Series A no. 20, p. 18, para. 50; see also the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, p. 46, para. 95). The Court proposes in the present case to decide on the applicability of Article 13 (art. 13), before examining, if necessary, the effectiveness of any relevant remedy under German law.

64. Article 13 (art. 13) states that any individual whose Convention rights and freedoms are violated is to have an effective remedy before a national authority even where the violation has been committed by persons in an official capacity. This provision, read literally, seems to say that a person is entitled to a national remedy only if a "violation" has occurred. However, the person cannot establish a "violation" before a national authority unless he is first able to lodge with such an authority a complaint to that effect. Consequently, as the minority in the Commission stated, it cannot be a prerequisite for the application of Article 13 (art. 13) that the Convention be in fact violated. In the Court's view, Article 13 (art. 13) requires that where an individual considers himself to have been prejudiced by a measure allegedly in breach of the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress. Thus Article 13 (art. 13) must be interpreted as guaranteeing an "effective remedy before a national authority" to everyone who claims that his rights and freedoms under the Convention have been violated.

65. Accordingly, although the Court has found no breach of the right guaranteed to the applicants by Article 8 (art. 8), it falls to be ascertained whether German law afforded the applicants an "effective remedy before a national authority" within the meaning of Article 13 (art. 13). The applicants are not claiming that, in relation to particular surveillance measures actually applied to them, they lacked an effective remedy for alleged violation of their rights under the Convention. Rather, their complaint is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing whether their rights under the Convention have been interfered with by such a concrete measure, is directed against what they consider to be a shortcoming in the content of the contested legislation. While conceding that some forms of recourse exist in certain circumstances, they contend that the legislation itself since it prevents them from even knowing
71. On the other hand, in pursuance of the Federal Constitutional Court’s judgment of 15 December 1970, the competent authority is bound to inform the person concerned as soon as the surveillance measures are discontinued and notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above). From the moment of such notification, various legal remedies - before the courts - become available to the individual. According to the information supplied by the Government, the individual may: in an action for a declaration, have reviewed by an administrative court the lawfulness of the application to him of the G 10 and the conformity with the law of the surveillance measures ordered; bring an action for damages in a civil court if he has been prejudiced; bring an action for the destruction or, if appropriate, restitution of documents; finally, if none of these remedies is successful, apply to the Federal Constitutional Court for a ruling as to whether there has been a breach of the Basic Law (see paragraph 24 above).

72. Accordingly, the Court considers that, in the particular circumstances of this case, the aggregate of remedies provided for under German law satisfies the requirements of Article 13 (art. 13).

IV. ON THE ALLEGED VIOLATION OF ARTICLE 6 PARA. 1 (art. 6-1)

73. The applicants finally alleged a breach of Article 6 para. 1 (art. 6-1) which provides: "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

74. According to the applicants, the surveillance measures which can be taken under the contested legislation amount both to an interference with a "civil right", and to the laying of a "criminal charge" within the meaning of Article 6 para. 1 (art. 6-1). In their submission, the legislation violates this Article (art. 6-1) in so far as it does not require notification to the person concerned in all cases after the termination of surveillance measures and excludes recourse to the courts to test the lawfulness of such measures. On the other hand, both the Government and the Commission concur in thinking that Article 6 para. 1 (art. 6-1) does not apply to the facts of the case under either the "civil" or the "criminal" head.

75. The Court has held that in the circumstances of the present case the G 10 does not contravene Article 8 (art. 8) in authorising a secret surveillance of mail, post and telecommunication subject to the conditions specified (see paragraphs 39 to 60 above). Since the Court has arrived at this conclusion, the question whether the decisions authorising such surveillance under the G 10 are covered by the judicial guarantee set forth in Article 6 (art. 6) – assuming this Article (art. 6) to be applicable - must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance. As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6 (art. 6); as a consequence, it of necessity escapes the requirements of that Article.

The decision can come within the ambit of the said provision only after discontinuance of the surveillance. According to the information supplied by the Government, the individual concerned, once he has been notified of such discontinuance, has at his disposal several legal remedies against the possible infringements of his rights; these remedies would satisfy the requirements of Article 6 (art. 6) (see paragraphs 24 and 71 above). The Court accordingly concludes that, even if it is applicable, Article 6 (art. 6) has not been violated.

FOR THESE REASONS, THE COURT

1. holds unanimously that it has jurisdiction to rule on the question whether the applicants can claim to be victims within the meaning of Article 25 (art. 25) of the Convention;

2. holds unanimously that the applicants can claim to be victims within the meaning of the aforesaid Article (art. 25);

3. holds unanimously that there has been no breach of Article 8, Article 13 or Article 6 (art. 8, art. 13, art. 6) of the Convention.

[–]

SEPARATE OPINION OF JUDGE PINHEIRO FARINHA
(Translation)

1. I agree with the judgment’s conclusions, but on different grounds.

1. The G 10 Act specifies, in Article 1 para. 1, the cases in which the competent authorities may impose restrictions, that is to say, may open and inspect mail and post, read telegraphic messages, listen to and record telephone conversations. It empowers those authorities so to act, inter alia, in order to protect against "imminent dangers" threatening the "free democratic constitutional order", "the existence or the security of the Federation or of a Land", "the security of the (allied) armed forces" stationed on the territory of the Republic and the security of "the troops of one of the Three Powers stationed in the Land of Berlin". According to Article 1 para. 2, these measures may be taken only where there are factual indications (tatsächliche Anhaltspunkte) for suspecting a person of planning, committing, or having committed certain criminal acts punishable under the Criminal Code, such as offences against the peace or security of the State (sub-paragraph 1, no. 1), the democratic order (sub-paragraph 1, no. 2), external security (sub-paragraph 1, no. 3) and the security of the allied armed forces (sub-paragraph 1, no. 5) (see paragraph 17 of the judgment).

For all those purposes, both the Government and the Commission agree that the G 10 can be applied, the mere fact of its existence creates a very real menace that their exercise of the right to respect for their private and family life and their correspondence may be the subject of surveillance. Clearly, therefore, a person may claim to be a victim for the purposes of Article 25 (art. 25) of the Convention. Consequently, the applicants have a direct interest (Jose Alberto dos Reis, Código do Processo Civil Anotado, vol. 1, p. 77), which is an ideal condition (Carnelutti, Sistema del diritto processuale civile, vol. 1, pp. 361 and 366) for an application to the Commission.

In my view, the applicants are the victims of a menace and for this reason can claim to be victims within the meaning of Article 25 (art. 25).

2. I would mention in passing one point of concern, namely, that the majority opinion, contained in paragraph 77, could take the interpretation of Article 8 (art. 8) in a direction which, if I may say so, might not be without risk. The measures are ordered, on written application giving reasons, either by the supreme Land authority in cases falling within its jurisdiction or by a Federal Minister empowered for the purpose by the Chancellor. The Chancellor has entrusted these functions to the Ministers of the Interior and of Defence,
each of whom, in the sphere falling within his competence, must personally take the decision as to the application of the measures (Article 1 para. 5, sub-paragraphs 1 and 2) (see paragraph 18 of the judgment).

Implementation of the measures ordered is supervised by an official qualified for judicial office (Article 1 para. 7, sub-paragraph 1) (see paragraph 20 of the judgment).

I believe that separation of powers is a basic principle of a democratic society and that, since the measures can be ordered where there are mere factual indications that criminal acts are about to be or are in the course of being committed, this principle requires that the measures be ordered by an independent judge - as was in fact contemplated by the German legislature (see paragraph 22 of the judgment).

I have difficulty in accepting that the political authority may decide by itself whether there exist factual indications that criminal acts are about to be or are in the course of being committed.

3. Acting in the general interest, the States, as the High Contracting Parties, safeguard the Convention against any breaches attributable to another State; such breaches can consist in the danger and threat to democracy which the publication of a law in itself may pose.

In cases originating in an application by individuals, it is necessary to show, in addition to the threat or danger, that there has been a specific violation of the Convention of which they claim to be the victims.

There is no doubt that a law can in itself violate the rights of an individual if it is directly applicable to that individual without any specific measure of implementation. This is the case with a law which denies those who reside in a particular area access to certain educational establishments, and with a law which makes sex education one of the compulsory subjects on the curriculum: these laws are applicable without the need for any implementing measure (see the "Belgian Linguistic" case and the Kjeldsen, Busk Madsen and Pedersen case).

The same does not hold true for the German G 10. The Act certainly makes provision for telephone-tapping and inspection of mail, although it delimits the scope of such measures and regulates the methods of enforcing them.

Surveillance of an "exploratory" or general kind is not, however, authorised by the legislation in question. If it were, then the Act would be directly applicable. Instead, the measures cannot be applied without a specific decision by the supreme Land authority or the competent Federal Minister who must, in addition, consider whether there exist any factual indications that a criminal act is about to be or is in the course of being committed.

This is only where a surveillance measure has been authorised and taken against a given individual does any question arise of an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence.

So far as the case sub judice is concerned, on the one hand, the applicants do not know whether the G 10 has in fact been applied to them (see paragraph 12 of the judgment) and, on the other hand, the respondent Government state - and we have no reason to doubt this statement - that "at no time have they been subjected to surveillance by mistake - for example through confusion over a telephone number -, since in such cases the person concerned is notified of the surveillance measure" (see paragraph 13 of the judgment).

The Court may take into consideration only the case of the applicants (Engel and others judgment of 8 June 1976, Series A no. 22, p. 43, para. 106) and not the situation of other persons not having authorised them to lodge an application with the Commission in their name.

These are the reasons which lead me to conclude, as the Court does, that the case sub judice does not disclose any violation of the Convention.

CASE OF MALONE v. THE UNITED KINGDOM
(Application no. 8691/79)

JUDGMENT
STRASBOURG
2 August 1984

[...]

PROCEDURE
1. The present case was referred to the Court by the European Commission of Human Rights ("the Commission") on 16 May 1983, within the period of three months laid down by Article 32 para. 1 and Article 47 (art. 32-1, art. 47) of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention"). The case originated in an application (no. 8691/79) against the United Kingdom of Great Britain and Northern Ireland lodged with the Commission on 19 July 1979 under Article 25 (art. 25) by a United Kingdom citizen, Mr. James Malone.

[...]

AS TO THE FACTS
1. PARTICULAR CIRCUMSTANCES OF THE CASE
12. Mr. James Malone was born in 1937 and is resident in Dorking, Surrey. In 1977, he was an antique dealer. It appears that he has since ceased business as such.

13. On 22 March 1977, Mr. Malone was charged with a number of offences relating to dishonest handling of stolen goods. His trial, which took place in June and August 1978, resulted in his being acquitted on certain counts and the jury disagreeing on the rest. He was retried on the remaining charges between April and May 1979. Following a further failure by the jury to agree, he was once more formally arraigned; the prosecution offered no evidence and he was acquitted.

14. During the first trial, it emerged that details of a telephone conversation to which Mr. Malone had been a party prior to 22 March 1977 were contained in the note-book of the police officer in charge of the investigations. Counsel for the prosecution then accepted that this conversation had been intercepted on the authority of a warrant issued by the Secretary of State for the Home Department.

15. In October 1978, the applicant instituted civil proceedings in the Chancery Division of the High Court against the Metropolitan Police Commissioner, seeking, inter alia, declarations to the effect that interception, monitoring and recording of conversations on his telephone line without his consent was unlawful, even if done pursuant to a warrant of the Secretary of State. The Solicitor General intervened in the proceedings on behalf of the Secretary of State but without being made a party. On 28 February 1979, the Vice-Chancellor, Sir Robert Megarry, dismissed the applicant's claim (Malone v. Commissioner of Police of the Metropolis [No. 2] [1979] 2 All England Law Reports 620; also reported at [1979] 2 Weekly Law Reports 700). An account of this judgment is set out below (at paragraphs 31-36).

16. The applicant further believed that both his correspondence and his telephone calls had been intercepted...
for a number of years. He based his belief on delay to and signs of interference with his correspondence. In particular, he produced to the Commission bundles of envelopes which had been delivered to him either sealed with an adhesive tape of an identical kind or in an unsealed state. As to his telephone communications, he stated that he had heard unusual noises on his telephone and alleged that the police had at times been in possession of information which they could only have obtained by telephone tapping. He thought that such measures had continued since his acquittal on the charges against him.

It was admitted by the Government that the single conversation about which evidence emerged at the applicant’s trial had been intercepted on behalf of the police pursuant to a warrant issued under the hand of the Secretary of State for the prevention and detection of crime. According to the Government, this interception was carried out in full conformity with the law and the relevant procedures. No disclosure was made either at the trial of the applicant or during the course of the applicant’s proceedings against the Commissioner of Police as to whether the applicant’s own telephone number had been tapped or as to whether other and, if so, what other, telephone conversations to which the applicant was a party had been intercepted. The primary reasons given for withholding this information were that disclosure would or might frustrate the purpose of telephone interceptions and might also serve to identify other sources of police information, particularly police informants, and thereby place at risk the source in question. For similar reasons, the Government declined to disclose before the Commission or the Court to what extent, if at all, the applicant’s telephone calls and correspondence had been intercepted on behalf of the police authorities. It was however denied that the rescaling with adhesive tape or the delivery unsealed of the envelopes produced to the Commission was attributable directly or indirectly to any interception. The Government conceded that, as the applicant was at the material time suspected by the police of being concerned in the receiving of stolen property and in particular of stolen antiques, he was one of a class of persons against whom measures of interception were liable to be employed.

17. In addition, Mr. Malone believed that his telephone had been “metered” on behalf of the police by a device which automatically records all numbers dialed. As evidence for this belief, he was charged in March 1977 that he had recently telephoned numbers searched by the police. The Government affirmed that the police had neither caused the applicant’s telephone calls to be metered nor undertaken the alleged or any search operations on the basis of any list of numbers obtained from metering.

18. In September 1978, the applicant requested the Post Office and the complaints department of the police to remove suspected listening devices from his telephone. The Post Office and the police both replied that they had no authority in the matter.

II. RELEVANT LAW AND PRACTICE

A. Introduction

19. The following account is confined to the law and practice in England and Wales relating to the interception of communications on behalf of the police for the purposes of the prevention and detection of crime. The expression “interception” is used to mean the obtaining of information about the contents of a communication by post or telephone without the consent of the parties involved.

20. It has for long been the practice for the interception of postal and telephone communications in England and Wales to be carried out on the authority of a warrant issued by a Secretary of State, nowadays normally the Secretary of State for the Home Department (the Home Secretary). There is no overall statutory code governing the matter, although various statutory provisions are applicable thereto. The effect in domestic law of these provisions is the subject of some dispute in the current proceedings. Accordingly, the present summary of the facts is limited to what is undisputed, the submissions in relation to the contested aspects of these provisions being dealt with in the part of the judgment “as to the law”.

21. Three official reports available to the public have described and examined the working of the system for the interception of communications.

Firstly, a Committee of Privy Councillors under the chairmanship of Lord Birkett was appointed in June 1957 “to consider and report upon the exercise by the Secretary of State of the executive power to intercept communications and, in particular, under what authority, to what extent and for what purposes this power has been exercised and to what use information so obtained has been put; and to recommend whether, how and subject to what safeguards, this power should be exercised ...”. The Committee’s report (hereinafter referred to as “the Birkett report”) was published in October 1957 (as Command Paper 283). The Government of the day announced that they accepted the report and its recommendations, and were taking immediate steps to implement those recommendations calling for a change in procedure. Subsequent Governments, in the person of the Prime Minister or the Home Secretary, publicly reaffirmed before Parliament that the arrangements relating to the interception of communications were strictly in accordance with the procedures described and recommended in the Birkett report.

Secondly, a Command Paper entitled “The Interception of Communications in Great Britain” was presented to Parliament by the then Home Secretary in April 1980 (Command Paper 7873 - hereinafter referred to as “the White Paper”). The purpose of the White Paper was to bring up to date the account given in the Birkett report.

Finally, in March 1981 a report by Lord Diplock, a Lord of Appeal in Ordinary who had been appointed to monitor the relevant procedures on a continuing basis (see paragraphs 54 and 55 below), was published outlining the results of the monitoring he had carried out to date.

22. The legal basis of the practice of intercepting telephone communications was also examined by the Vice-Chancellor in his judgment in the action which the applicant brought against the Metropolitan Police Commissioner (see paragraphs 31-36 below).

23. Certain changes have occurred in the organisation of the postal and telephone services since 1957, when the Birkett Committee made its report. The Post Office, which ran both services, was then a Department of State under the direct control of a Minister (the Postmaster General). By virtue of the Post Office Act 1969, it became a public corporation with a certain independence of the Crown, though subject to various ministerial powers of supervision and control exercised at the material time by the Home Secretary. The Post Office Act 1969 was repealed in part and amended by the British Telecommunications Act 1981. That Act divided the Post Office into two corporations: the Post Office, responsible for mail, and British Telecommunications, responsible for telephones. The 1981 Act made no change of substance in relation to the law governing interceptions. For the sake of convenience, references in the present judgment are to the position as it was before the 1981 Act came into force.

24. The existence of a power vested in the Secretary of State to authorise by warrant the interception of correspondence, in the sense of detaining and opening correspondence
transmitted by post, has been acknowledged from early times and its exercise has been publicly known (see the Birkett report, Part I, especially paras. 11, 17 and 39). The precise origin in law of this executive authority is obscure (ibid., para. 9). Nevertheless, although none of the Post Office statutes (of 1710, 1837, 1908 or 1953) contained clauses expressly conferring authority to intercept communications, all recognised the power as an independently existing power which it was lawful to exercise (ibid., paras. 17 and 38).

25. At the time of the Birkett report, the most recent statutory provision recognising the right of interception of a postal communication was section 58 sub-section 1 of the Post Office Act 1953, which provides:

"If any officer of the Post Office, contrary to his duty, opens ... any such postal packet, he shall be guilty of a misdemeanour ..."

Provided that nothing in this section shall extend to ... the opening, detaining or delaying of a postal packet ... in obedience to an express warrant in writing under the hand of a Secretary of State."

"Postal packet" is defined in section 87 sub-section 1 of the Act as meaning:

"a letter, postcard, reply postcard, newspaper, printed packet, sample packet or parcel and every packet or article transmissible by post, and includes a telegram."

Section 58, which is still in force, reproduced a clause that had been on the statute book without material amendment since 1710.

26. So far as telecommunications are further concerned, it is an offence under section 45 of the Telegraph Act 1863 if an official of the Post Office "improperly divulges to any person the purport of any message". Section 11 of the Post Office (Protection) Act 1884 creates a similar offence in relation to telegrams. In addition, section 20 of the Telegraph Act 1868 makes it a criminal offence if any Post Office official "shall, contrary to his duty, disclose or in any way make known or intercept the contents or any part of the contents of any telegraphic message or any message entrusted to the [Post Office] for the purpose of transmission".

These provisions are still in force.

27. It was held in a case decided in 1880 (Attorney General v. Edison Telephone Company, (1880) 6 Queen's Bench Division 244) that a telephone conversation is a "telegraphic communication" for the purposes of the Telegraph Acts. It has not been disputed in the present proceedings that the offences under the Telegraph Acts apply to telephone conversations.

28. The power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone. Until the year 1937, the Post Office, which was at that time a Department of Government, acted upon the view that the power which the Crown exercised in intercepting telephone messages was a power possessed by any operator of telephones and was not contrary to law. Consequently, no warrants by the Secretary of State were issued and arrangements for the interception of telephone conversations were made directly between the police authorities and the Director-General of the Post Office. In 1937, the position was reviewed by the Home Secretary and the Postmaster General (the Minister then responsible for the administration of the Post Office) and it was decided, as a matter of policy, that it was undesirable that records of telephone conversations should be made by Post Office servants and disclosed to the police without the authority of the Secretary of State. The view was taken that the power which had for long been exercised to intercept postal communications on the authority of a warrant of the Secretary of State was, by its nature, wide enough to include the interception of telephone communications. Since 1937 it had accordingly been the practice of the Post Office to intercept telephone conversations only on the express warrant of the Secretary of State (see the Birkett report, paras. 40-41).

The Birkett Committee considered that the power to intercept telephone communications rested upon the power plainly recognised by the Post Office statutes as existing before the enactment of the statutes (Birkett report, para. 50). It concluded (ibid., para. 51):

"We are therefore of the opinion that the state of the law might fairly be expressed in this way.

(a) The power to intercept letters has been exercised from the earliest times, and has been recognised in successive Acts of Parliament.

(b) This power extends to telegrams.

(c) It is difficult to resist the view that if there is a lawful power to intercept communications in the form of letters and telegrams, then it is wide enough to cover telephone communications as well."

C. Post Office Act 1969

29. Under the Post Office Act 1969, the "Post Office" ceased to be a Department of State and was established as a public corporation of that name with the powers, duties and functions set out in the Act. In consequence of the change of status of the Post Office and of the fact that the Post Office was no longer under the direct control of a Minister of the Crown, it became necessary to make express statutory provision in relation to the interception of communications on the authority of a warrant of the Secretary of State. By section 80 of the Act it was therefore provided as follows:

"A requirement to do what is necessary to inform designated persons holding office under the Crown concerning matters and things transmitted or in course of transmission by means of postal or telecommunication services provided by the Post Office may be laid on the Post Office for the like purposes and in the like manner as, at the passing of this Act, a requirement may be laid on the Postmaster General to do what is necessary to inform such persons concerning matters and things transmitted or in course of transmission by means of such services provided by him."

30. The 1969 Act also introduced, for the first time, an express statutory defence to the offences under the Telegraph Acts mentioned above (at paragraph 26), similar to that which exists under section 58 para. 1 of the Post Office Act 1953. This was effected by paragraph 1 sub-paragraph 1 of Schedule 5 to the Act, which reads:

"In any proceedings against a person in respect of an offence under section 45 of the Telegraph Act 1863 or section 11 of the Post Office (Protection) Act 1884 consisting in the improper divulging of the purport of any message or any part of it, he shall be entitled to rely for a defence in such proceedings on evidence that the act constituting the offence was done in obedience to a warrant of the Secretary of State."

D. Judgment of Sir Robert Megarry V.-C. in Malone v. Commissioner of Police of the Metropolis

31. In the civil action which he brought against the Metropolitan Police Commissioner, Mr. Malone sought various relief including declarations to the following effect:

- that any "tapping" (that is, interception, monitoring or recording) of conversations on his telephone lines without his consent, or disclosing the contents thereof, was unlawful even if done pursuant to a warrant of the Home Secretary;
- that he had rights of property, privacy and confidentiality in respect of conversations on his telephone lines and that the above-stated tapping and disclosure were in breach of those rights;
- that the tapping of his telephone lines violated Article 8 (art. 8) of the Convention.

In his judgment, delivered on 28 February 1979, the Vice-Chancellor noted that he had no jurisdiction to make the
I am not concerned with is the legality of tapping effected by means of recording telephone conversations from wires which, though connected to the premises of the subscriber, are not on them.” ([1979] 2 All England Law Reports, p. 629).

33. The Vice-Chancellor held that there was no right of property (as distinct from copyright) in words transmitted along telephone lines (ibid., p. 631). As to the remaining contentions based on privacy and confidentiality, he observed firstly that no assistance could be derived from cases dealing with other kinds of warrant. Unlike a search of premises, the process of telephone tapping on Post Office premises did not involve any act of trespass and so was not prima facie illegal (ibid., p. 640). Secondly, referring to the warrant of the Home Secretary, the Vice-Chancellor remarked that such warrant did not “purport to be issued under the authority of any statute or of the common law”. The decision to introduce such warrants in 1937 seemed “plainly to have been an administrative decision not dictated or required by statute” (ibid.). He referred, however, to section 80 of the Post Office Act 1969 and Schedule 5 to the Act, on which the Solicitor General had based certain contentions summarised as follows:

“Although the previous arrangements had been merely administrative, they had been set out in the Birkett report a dozen years earlier, and the section plainly referred to these arrangements: ... A warrant was not needed to make the tapping lawful: it was lawful without any warrant. But where the tapping was done under warrant ... [section 80] afforded statutory recognition of the lawfulness of the tapping.” (ibid., p. 641)

“In their essentials”, stated the Vice-Chancellor, “these contentions seem to me to be sound.” He accepted that, by the 1969 Act, “Parliament has provided a clear recognition of the warrant of the Home Secretary as having an effective function in law, both as providing a defence to certain criminal charges, and also as amounting to an effective requirement for the Post Office to do certain acts” (ibid., pp. 641-642).

The Vice-Chancellor further concluded that there was in English law neither a general right of privacy nor, as the applicant had contended, a particular right of privacy to hold a telephone conversation in the privacy of one’s home without molestation (ibid., pp. 642-644). Moreover, no duty of confidentiality existed between the Post Office and the telephone subscriber; nor was there any other obligation of confidence on a person who overheard a telephone conversation, whether by means of tapping or otherwise (ibid., pp. 645-647).

He then considered the applicant’s argument that the Convention, as interpreted by the European Court in the case of Klass and Others (judgment of 6 September 1978, Series A no. 28), could be used as a guide to assist in the determination of English law on a point that was uncertain. He observed that the issues before him did not involve construing legislation enacted with the purpose of giving effect to obligations imposed by the Convention. Where Parliament had abstained from legislating on a point that was plainly suitable for legislation, it was difficult for the court to lay down new rules that would carry out the Crown’s treaty obligations, or to discover for the first time that such rules had always existed. He compared the system of safeguards considered in the Klass case with the English system, as described in the Birkett report, and concluded:

“... Not a single one of these safeguards is to be found as a matter of established law in England, and only a few corresponding provisions exist as a matter of administrative procedure.

It does not, of course, follow that a system with fewer or different safeguards will fail to satisfy Article 8 (art. 8) in the eyes of the European Court of Human Rights. At the same time, it is impossible to read the judgment in the Klass case without it becoming abundantly clear that a system which has no legal safeguards whatever has small chance of satisfying the requirements of that Court, whatever administrative provisions there may be. ... Even if the system [in operation in England] were to be considered adequate in its conditions, it is laid down merely as a matter of administrative procedure, so that it is unenforceable in law, and as a matter of law could at any time be altered without warning or subsequent notification. Certainly in law any ‘adequate and effective safeguards against abuse’ are wanting. In this respect English law compares most unfavourably with West German law: this is not a subject on which it is possible to feel any pride in English law.

I therefore find it impossible to see how English law could be said to satisfy the requirements of the Convention, as interpreted in the Klass case, unless that law not only prohibited all telephone tapping save in suitably limited classes of case, but also laid down detailed restrictions on the exercise of the power in those limited classes.”

This conclusion did not, however, enable the Vice-Chancellor to decide the case in the way the applicant sought:

"It may perhaps be that the common law is sufficiently fertile to achieve what is required by the first limb of [the above-stated proviso]: possible ways of expressing such a rule may be seen in what I have already said. But I see the greatest difficulty in the common law framing the safeguards required by the second limb. Various institutions or offices would have to be brought into being to exercise various defined functions. The more complex and indefinite the subject-matter the greater the difficulty in the court doing what it is really appropriate, and only appropriate, for the legislature to do. Furthermore, I find it hard to see what there is in the present case to require the English courts to struggle with such a problem. Give full rein to the Convention, and it is clear that when the object of the surveillance is the detection of crime, the question is not whether there ought to be a general prohibition of all surveillance, but in what circumstances, and subject to what conditions and restrictions, it ought to be permitted. It is in these circumstances and conditions and restrictions which are at the centre of this case; and yet it is they which are the least suitable for determination by judicial decision.

... Any regulation of so complex a matter as telephone tapping is essentially a matter for Parliament, not the courts; and neither the Convention nor the Klass case can, I think, play any proper part in deciding the issue before me.” (ibid., pp. 647-649)

He added that “this case seems to me to make it plain that telephone tapping is a subject which cries out for legislation”, and continued:
"However much the protection of the public against crime demands that in proper cases the police should have the assistance of telephone tapping, I would have thought that in any civilised system of law the claims of liberty and justice would require that telephone users should have effective and independent safeguards against possible abuses. The fact that a telephone user is suspected of crime increases rather than diminishes this requirement: suspicions, however reasonably held, may sometimes prove to be wholly unfounded. If there were effective and independent safeguards, these would not only exclude some cases of excess, but also, by their mere existence, provide some degree of reassurance for those who are resentful of the police or believe themselves to be persecuted.” (ibid., p. 649)

35. As a final point of substance, the Vice-Chancellor dealt, in the following terms, with the applicant’s contention that as no power to tap telephones had been given by either statute or common law, the tapping was necessarily unlawful: "I have already held that, if such tapping can be carried out without committing any breach of the law, it requires no authorisation by statute or common law; it can lawfully be done simply because there is nothing to make it unlawful. Now that I have held that such tapping can indeed be carried out without committing any breach of the law, the contention necessarily fails. I may also say that the statutory recognition given to the Home Secretary’s warrant seems to me to point clearly to the same conclusion." (ibid., p. 649)

36. The Vice-Chancellor therefore held that the applicant’s claim failed in its entirety. He made the following concluding remarks as to the ambit of his decision: "Though of necessity I have discussed much, my actual decision is closely limited. It is confined to the tapping of the telephone lines of a particular person which is effected by the Post Office on Post Office premises in pursuance of a warrant of the Home Secretary in a case in which the police have just cause or excuse for requesting the tapping, in that it will assist them in performing their functions in relation to crime, whether in prevention, detection, discovery of the criminals or otherwise, and in which the material obtained is used only by the police, and only for those purposes. In particular, I decide nothing on tapping effected for other purposes, or by other persons, or by other means; nothing on tapping when the information is supplied to persons other than the police; and nothing on tapping when the police use the material for purposes other than those I have mentioned. The principles involved in my decision may or may not be of some assistance in such other cases, whether by analogy or otherwise: but my actual decision is limited in the way that I have just stated." (ibid., p. 651)

E. Subsequent consideration of the need for legislation

37. Following the Vice-Chancellor’s judgment, the necessity for legislation concerning the interception of communications was the subject of review by the Government, and of Parliamentary discussion. On 1 April 1980, on the publication of the White Paper, the Home Secretary announced in Parliament that after carefully considering the suggestions proffered by the Vice-Chancellor in his judgment, the Government had decided not to introduce legislation. He explained the reasons for this decision in the following terms: "The interception of communications is, by definition, a practice that depends for its effectiveness and value upon being carried out in secret, and cannot therefore be subject to the normal processes of parliamentary control. Its acceptability in a democratic society depends on its being subject to ministerial control, and on the readiness of the public and their representatives in Parliament to repose their trust in the Ministers concerned to exercise that control responsibly and with a right sense of balance between the value of interception as a means of protecting order and security and the threat which it may present to the liberty of the subject. Within the necessary limits of secrecy, I and my right hon. Friends who are concerned are responsible to Parliament for our stewardship in this sphere. There would be no more sense in making such secret matters justiciable than there would be in my being obliged to reveal them in the House. If the power to intercept were to be regulated by statute, then the courts would have power to inquire into the matter and to do so, if not publicly, then at least in the presence of the complainant. This would provide some interception as a tool of investigation. The Government have come to the clear conclusion that the procedures, conditions and safeguards described in the White Paper ensure strict control of interception by Ministers, are a good and sufficient protection for the liberty of the subject, and would not be made significantly more effective for that purpose by being embodied in legislation. The Government have accordingly decided not to introduce legislation on these matters" (Hansard, House of Commons, 1 April 1980, cols. 205-207).

He gave an assurance that "Parliament will be informed of any changes that are made in the arrangements" (ibid., col. 208).

38. In the course of the Parliamentary proceedings leading to the enactment of the British Telecommunications Act 1981, attempts were made to include in the Bill provisions which would have made it an offence to intercept mail or matters sent by public telecommunication systems. Despite this, the Government successfully opposed these moves, primarily on the grounds that secrecy, which was essential if interception was to be effective, could not be maintained if the arrangements for interception were laid down by legislation and thus became justiciable in the courts. The present arrangements and safeguards were adequate and the proposed new provisions were, in the Government’s view, unworkable and unnecessary (see, for example, the statement of the Home Secretary in the House of Commons on 1 April 1981, Hansard, cols. 334-338). The 1981 Act eventually contained a re-enactment of section 80 of the Post Office Act 1969 applicable to the Telecommunications Corporation (Schedule 3, para. 1, of the 1981 Act). Section 80 of the 1969 Act itself continues to apply to the Post Office.

39. In its report presented to Parliament in January 1981 (Command Paper 8092), the Royal Commission on Criminal Procedure, which had been appointed in 1978, also considered the possible need for legislation in this field. In the chapter entitled "Investigative powers and the rights of the citizen", the Royal Commission made the following recommendation in regard to what it termed "surreptitious surveillance" (para. 3.56-3.60): 

"… [A]lthough we have no evidence that the existing controls are inadequate to prevent abuse, we think that there are strong arguments for introducing a system of statutory control on similar lines to that which we have recommended for search warrants. As with all features of police investigative procedures, the value of prescribing them in statutory form is that it brings clarity and precision to the rules; they are open to public scrutiny and to the potential of Parliamentary review. So far as surveillance devices in general are concerned this is not at present so.

We therefore recommend that the use of surveillance devices by the police (including the interception of letters and telephone communications) should be regulated by statute.” These recommendations were not adopted by the Government.

40. A few months later, the Law Commission, a permanent body set up by statute in 1965 for the purpose of promoting reform of the law, produced a report on breach of confidence (presented to Parliament in October 1981 - Command Paper..."
This report examined, inter alia, the implications for the civil law of confidence of the acquisition of information by surveillance devices, and made various proposals for reform of the law (paras. 6.35 - 6.46). The Law Commission, however, felt that the question whether "the methods which the police ... may use to obtain information should be defined by statute" was a matter outside the scope of its report (paras. 6.43 and 6.44 in fine). No action has been taken by the Government on this report.

F. The practice followed in relation to interceptions


42. The police, H.M. Customs and Excise and the Security Service may request authority for the interception of communications for the purposes of "detected serious crime and the safeguarding of the security of the State" (paragraph 2 of the White Paper). Interception may take place only on the authority of the Secretary of State given by warrant under his own hand. In England and Wales, the power to grant such warrants is exercised by the Home Secretary or occasionally, if he is ill or absent, by another Secretary of State on his behalf (ibid.). In the case of warrants applied for by the police to assist them in the detection of crime, three conditions must be satisfied before a warrant will be issued:

(a) the offence must be "really serious";
(b) normal methods of investigation must have been tried and failed or must, from the nature of things, be unlikely to succeed;
(c) there must be good reason to think that an interception would be likely to lead to an arrest and a conviction.

43. As is indicated in the Birkett report (paras. 58-61), the concept of "serious crime" has varied from time to time. Changing circumstances have made some acts serious offences which were not previously so regarded; equally, some offences formerly regarded as serious enough to justify warrants for the interception of communications have been regarded. Thus, the interception of letters believed to contain obscene or indecent matter ceased in the mid-1950s (Birkett report, para. 60); no warrants for the purpose of preventing the transmission of illegal lottery material have been issued since November 1953 (ibid., para. 59). "Serious crime" is defined in the White Paper, and the concluding words has been consistently defined since September 1951 (Birkett report, para. 64), as consisting of "offences for which a man with no previous record could reasonably be expected to be sentenced to three years' imprisonment, or offences of lesser gravity in which either a large number of people is involved or there is good reason to apprehend the use of violence" (White Paper, para. 4).

In April 1982, the Home Secretary announced to Parliament that, on a recommendation made by Lord Diplock in his second report (see paragraph 55 below), the concept of a serious offence was to be extended to cover offences which would not necessarily attract a penalty of three years' imprisonment on first conviction, but in which the financial rewards of success were very large (Hansard, House of Commons, 21 April 1982, col. 95).

Handling (including receiving) stolen goods, knowing or believing them to be stolen, is an offence under section 22 of the Theft Act 1968, carrying a maximum penalty of fourteen years' imprisonment. According to the Government, the receiving of stolen property is regarded as a very serious offence since the receiver lies at the root of much organised crime and encourages large-scale thefts (see the Birkett report, para. 103). The detection of receivers of stolen property was at the time of the Birkett report (ibid.), and remains, one of the important uses to which interception of communications is put by the police.

44. Applications for warrants must be made in writing and must contain a statement of the purpose for which interception is requested and of the facts and circumstances which support the request. Every application is submitted to the Permanent Under-Secretary of State - the senior civil servant - at the Home Office (or, in his absence, a nominated deputy), who, if he is satisfied that the application meets the required criteria, submits it to the Secretary of State for approval and signature of a warrant. In a case of exceptional urgency, if the Secretary of State is not immediately available to sign a warrant, he may be asked to give authority orally, by telephone; a warrant is signed and issued as soon as possible thereafter (White Paper, para. 9).

In their submissions to the Commission and the Court, the Government supplemented as follows the information given in the White Paper. Except in cases of exceptional urgency, an application will only be considered in the Home Office if it is put forward by a senior officer of the Metropolitan Police, in practice the Assistant Commissioner (Crime), and also, in the case of another police force, by the chief officer of police concerned. Close personal consideration is given by the Secretary of State to every request for a warrant submitted to him. In the debate on the British Telecommunications Bill in April 1981, the then Home Secretary confirmed before Parliament that he did not and would not sign any warrant for interception unless he were personally satisfied that the relevant criteria were met (Hansard, House of Commons, 1 April 1981, col. 336).

45. Every warrant sets out the name and address of the recipient of mail in question or the telephone number to be monitored, together with the name and address of the subscriber. Any changes require the authority of the Secretary of State, who may delegate power to give such authority to the Permanent Under-Secretary. If both the mail and telephone line of a person are to be intercepted, two separate warrants are required (White Paper, para. 10).

46. Every warrant is time-limited, specifying a date on which it expires if it is not renewed. Warrants are in the first place issued with a time-limit set at a defined date not exceeding two months from the date of issue. Warrants may be renewed only on the personal authority of the Secretary of State and may be renewed for not more than one month at a time. In each case where renewal of a warrant is sought, the police are required first to satisfy the Permanent Under-Secretary of State at the Home Office that the reasons for which the warrant was first issued are still valid and that the case for renewal is justified: a submission to the Secretary of State for authority to renew the warrant is only made if the Permanent Under-Secretary is so satisfied (White Paper, para. 11).

47. Warrants are reviewed monthly by the Secretary of State. When an interception is considered to be no longer necessary, it is immediately discontinued and the warrant is cancelled on the authority of the Permanent Under-Secretary of State at the Home Office. In addition to the monthly review of each warrant by the Secretary of State, the Metropolitan Police carry out their own review each month of all warrants arising from police applications: where an interception is deemed to be no longer necessary, instructions are issued to the Post Office to discontinue the interception forthwith and the Home Office is informed so that the warrant can be cancelled (Birkett report, paras. 72-74; White Paper, paras. 12-13).

48. In accordance with the recommendations of the Birkett report (para. 84), records are kept in the Home Office, showing in respect of each application for a warrant:

(a) the ground on which the warrant is applied for;
49. On the issue of a warrant, the interception is effected by the Post Office. Telephone interceptions are carried out by a small staff of Post Office employees who record the conversations but do not themselves listen to it except from time to time to ensure that the apparatus is working correctly. In the case of postal communications, the Post Office makes a copy of the correspondence. As regards the interception of communications for the purpose of the detection of crime, in practice the "designated person holding office under the Crown," to whom the Post Office is required by subsection 80 of the Post Office Act 1969 to transmit the intercepted information (see paragraph 29 above) is invariably the Commissioner of Police of the Metropolis. The product of the interception - that is, the copy of the correspondence or the tape-recording - is made available to a special unit of the Metropolitan Police who note or transcribe only such parts of the correspondence or the telephone conversation as are relevant to the investigation. When the documentary record has been made, the tape is returned to the Post Office staff, who erase the recording. The tape is subsequently re-used.

50. A Consolidated Circular to Police, issued by the Home Office in 1977, contained the following paragraphs in a section headed "Supply of information by Post Office to police":

1.67 Head Postmasters and Telephone Managers have been given authority to assist the police as indicated in paragraph 1.68 below without reference to Post Office Headquarters, in circumstances where the police are seeking information

(a) in the interests of justice in the investigation of a serious indictable offence; or

(b) when they are acting in a case on the instructions of the Director of Public Prosecutions; or

(c) when a warrant has been issued for the arrest of the offender, or the offence is such that he can be arrested without a warrant; or

1.68 Head Postmasters, or (in matters affecting the telecommunication service) Telephone Managers, may afford the following facilities in response to a request made by the officer locally in charge of the force at the town where the Head Postmaster is stationed

(g) Telegrams. Telegrams may be shown to the police on the authority of the sender or addressee. Apart from this the Post Office is prepared to give authority in particular cases of serious crime where the inspection of a telegram is a matter of urgency, and will do so at once on telephonic application, by a chief officer of police or a responsible officer acting on his behalf, to the Chief Inspector, Post Office Investigation Division.

1.69

1.70 As regards any matter not covered by paragraphs 1.67 and 1.68 above, if the police are in urgent need of information which the Post Office may be able to furnish in connection with a serious criminal offence, the police officer in charge of the investigation should communicate with the Duty Officer, Post Office Investigation Division who will be ready to make any necessary inquiries of other branches of the Post Office and to communicate any information which can be supplied."

In May 1984, the Home Office notified chief officers of police that paragraph 1.68 (g), described as containing advice and information to the police which was "in some respects misleading", was henceforth to be regarded as deleted, with the exception of the first complete sentence. At the same time, chief officers of police were reminded that the procedures for the interception of communications were set out in the White Paper and rigorously applied in all cases.

51. The notes or transcripts of intercepted communications are retained in the police interception unit for a period of twelve months or for as long as they may be required for the purposes of investigation. The contents of the documentary record are communicated to the officers of the appropriate police force engaging in the criminal investigation in question. When the notes or transcripts are no longer required for the purposes of the investigation, the documentary record is destroyed (Birkett report, para. 118; White Paper, para. 15).

The product of intercepted communications is used exclusively for the purpose of assisting the police to pursue their investigations; the material is not tendered in evidence, although the interception may itself lead to the obtaining of information by other means which may be tendered in evidence (Birkett report, para. 151; White Paper, para. 16). In accordance with the recommendation of the Birkett Committee (Birkett report, para. 101), information obtained by means of an interception is never disclosed to private individuals or private bodies or to courts or tribunals of any kind (White Paper, para. 17).

52. An individual whose communications have been intercepted is not informed of the fact of interception or of the information thereby obtained, even when the surveillance and the related investigations have terminated.

53. For security reasons it is the normal practice not to disclose the numbers of interceptions made (Birkett report, paras. 119-121; White Paper, paras. 24-25). However, in order to allay public concern as to the extent of interception, both the Birkett report and the White Paper gave figures for the number of warrants granted annually over the years preceding their publication. The figures in the White Paper (Appendix III) indicate that in England and Wales between 1969 and 1979 generally something over 400 telephone warrants and something under 100 postal warrants were granted annually by the Home Secretary. Paragraph 27 of the White Paper also gave the total number of Home Secretary warrants in force on 31 December for the years 1958 (237), 1968 (273) and 1978 (308). The number of telephones installed at the end of 1979 was, according to the Government, 26,428,000, as compared with 7,327,000 at the end of 1957. The Government further stated that over the period from 1958 to 1978 there was a fourfold increase in indictable crime, from 626,000 to 2,395,000.

54. When the White Paper was published on 1 April 1980, the Home Office announced in Parliament that the Government, whilst not proposing to introduce legislation (see paragraph 37 above), intended to appoint a senior member of the judiciary to conduct a continuous independent check so as to ensure that interception of communications was being carried out for the established purposes and in accordance with the established procedures. His terms of reference were stated to be:

"to review on a continuing basis the purposes, procedures, conditions and safeguards governing the interception of communications on behalf of the police, HM Customs and Excise and the security service as set out in [the White Paper]; and to report to the Prime Minister" (Hansard, House of Commons, 1 April 1980, cols. 207-208).

It was further announced that the person appointed would have the right of access to all relevant papers and the right to request additional information from the departments and organisations concerned. For the purposes of his first report, which would be published, he would examine all the arrangements set out in the White Paper; his subsequent reports on the detailed operation of the arrangements would not be published, but Parliament would be informed of any
findings of a general nature and of any changes that were made in the arrangements (ibid.).

55. Lord Diplock, a Lord of Appeal in Ordinary since 1968, was appointed to carry out the review. In his first report, published in March 1981, Lord Diplock recorded, inter alia, that, on the basis of a detailed examination of apparently typical cases selected at random, he was satisfied (i) that, in each case, the information provided by the applicant authorities to the Secretary of State in support of the issue of a warrant was stated with accuracy and candour and that the procedures followed within the applicant authorities for vetting applications before submission to the Secretary of State were appropriate to detect and correct any departure from proper standards; (ii) that warrants were not applied for save in proper cases and were not continued any longer than was necessary to carry out their legitimate purpose.

Lord Diplock further found from his examination of the system that all products of interception not directly relevant to the purpose for which the warrant was granted were speedily destroyed and that such material as was directly relevant to that purpose was given no wider circulation than was essential for carrying it out.

In early 1982, Lord Diplock submitted his second report. As the Secretary of State informed Parliament, Lord Diplock’s general conclusion was that during the year 1981 the procedure for the interception of communications had continued to work satisfactorily and the principles set out in the White Paper had been conscientiously observed by all departments concerned.

In 1982, Lord Diplock resigned his position and was succeeded by Lord Bridge of Harwich, a Lord of Appeal in Ordinary since 1980.

G. “Metering”

56. The process known as “metering” involves the use of a device called a meter check printer which registers the numbers dialled on a particular telephone and the time and duration of each call. It is a process which was designed by the Post Office for its own purposes as the corporation responsible for the provision of telephone services. Those purposes include ensuring that the subscriber is correctly charged, investigating complaints of poor quality service and checking possible abuse of the telephone service. When “metering” a telephone, the Post Office - now British Telecommunications (see paragraph 23 above) - makes use only of signals sent to itself.

In the case of the Post Office, the Crown does not require the keeping of records of this kind but, if the records are kept, the Post Office may be compelled to produce them in evidence in civil or criminal cases in the ordinary way, namely by means of a subpoena duces tecum. In this respect the position of the Post Office records of this kind but, if the records are kept, the Post Office may be compelled to produce them in evidence in civil or criminal cases in the ordinary way, namely by means of a subpoena duces tecum. In this respect the position of the Post Office records is no different from that of any other party holding relevant records as, for instance, a banker. Neither the police nor the Crown are empowered to direct or compel the production of the Post Office records otherwise than by the normal means.

However, the Post Office do on occasions make and provide such records at the request of the police if the information is essential to police enquiries in relation to serious crime and cannot be obtained from other sources. This practice has been made public in answer to parliamentary questions on more than one occasion (see, for example, the statement by the Home Secretary to Parliament, Hansard, House of Commons, 23 February 1978, cols. 760-761).

57. Commission, Government and applicant are agreed that, at least in theory, judicial remedies are available in England and Wales, in both the civil and the criminal courts, in respect of interceptions of communications carried out unlawfully. The remedies referred to by the Government were summarised in the pleadings as follows: (i) In the event of any interception or disclosure of intercepted material effectuated by a Post Office employee “contrary to duty” or “improperly” and without a warrant of the Secretary of State, a criminal offence would be committed under the Telegraph Acts 1863 and 1868 and the Post Office (Protection) Act 1884 (as regards telephone interceptions) and under the Post Office Act 1953 (as regards postal interceptions) (see paragraphs 25-27 above). On complaint that communications had been unlawfully intercepted, it would be the duty of the police to investigate the matter and to initiate a prosecution if satisfied that an offence had been committed. If the police failed to prosecute, it would be open to the complainant himself to commence a private prosecution. (ii) In addition to (i) above, in a case of unlawful interception by a Post Office employee without a warrant, an individual could obtain an injunction from the domestic courts to restrain the person or persons concerned and the Post Office itself from carrying out further unlawful interception of his communications: such an injunction is available to any person who can show that a private right or interest has been interfered with by a criminal act (see, for example, Gouriet v. The Union of Post Office Workers, [1977] 3 All England Law Reports 70; Ex parte Island Records Ltd., [1978] 3 All England Law Reports 795).

(iii) On the same grounds, an action would lie for an injunction to restrain the divulging or publication of the contents of intercepted communications by employees of the Post Office, otherwise than under a warrant of the Secretary of State, or to any person other than the police.

Besides these remedies, unauthorised interference with mail would normally constitute the tort of trespass to (that is, wrongful interference with) chattels and so give rise to a civil action for damages.

58. The Government further pointed to the following possible non-judicial remedies: (i) In the event that the police were themselves implicated in an interception carried out without a warrant, a complaint could additionally be lodged under section 49 of the Police Act 1964, which a chief officer of police would, by the terms of the Act, be obliged to investigate and, if an offence appeared to him to have been committed, to refer to the Director of Public Prosecutions. (ii) If a complaint were able to establish merely that the police or the Secretary of State had misappreciated the facts or that there was not an adequate case for imposing an interception, the individual concerned would be able to complain directly to the Secretary of State himself or through his Member of Parliament: if a complainant were to give the Home Secretary information which suggested that the grounds on which a warrant had been issued did not in fact fall within the published criteria or were inadequate or mistaken, the Home Secretary would immediately cause it to be investigated and, if the complaint were found to be justified, would immediately cancel the warrant. (iii) Similarly, if there were non-compliance with any of the relevant administrative rules of procedure set out in the Birkett report and the White Paper, a remedy would lie through complaint to the Secretary of State, who would, in a proper case, cancel or revoke a warrant and thereby terminate an interception which was being improperly carried out.

According to the Government, in practice there never has been a case where a complaint in any of the three above circumstances has proved to be well-founded.

[...]
FINAL SUBMISSIONS MADE TO THE COURT BY THE GOVERNMENT

61. At the hearings on 20 February 1984, the Government maintained the submissions set out in their memorial, whereby they requested the Court "[l] with regard to Article 8 (art. 8).

(i) to decide and declare that the interference with the exercise of the rights guaranteed by Article 8 para. 1 (art. 8-1) of the Convention resulting from the measures of interception of communications on behalf of the police in England and Wales for the purpose of the detection and prevention of crime, and any application of those measures to the applicant, were and are justified under paragraph 2 of Article 8 (art. 8-2) as being in accordance with the law and necessary in a democratic society for the prevention of crime and for the protection of the rights and freedoms of others and that accordingly there has been no breach of Article 8 (art. 8) of the Convention;

(ii) (a) to decide and declare that it is unnecessary in the circumstances of the present case to investigate whether the applicant's rights under Article 8 (art. 8) were interfered with by the so-called system of 'metering'; alternatively (b) to decide and declare that the facts found disclose no breach of the applicant's rights under Article 8 (art. 8) by reason of the said system of 'metering';

(2) with regard to Article 13 (art. 13).

to decide and declare that the circumstances of the present case disclose no breach of Article 13 (art. 13) of the Convention".

AS TO THE LAW

I. ALLEGED BREACH OF ARTICLE 8 (art. 8)

62. Article 8 (art. 8) provides as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." The applicant alleged violation of this Article (art. 8) under two heads. In his submission, the first violation resulted from interception of his postal and telephone communications by or on behalf of the police, or from the law and practice in England and Wales relevant thereto; the second from "metering" of his telephone by or on behalf of the police, or from the law and practice in England and Wales relevant thereto.

A. Interception of communications

1. Scope of the issue before the Court

63. It should be noted from the outset that the scope of the case before the Court does not extend to interception of communications in general. The Commission's decision of 13 July 1981 declaring Mr. Malone's application to be admissible determines the object of the case brought before the Court (see, inter alia, the Ireland v. the United Kingdom judgment of 18 January 1978, Series A no. 25, p. 63, para. 157). According to that decision, the present case "is directly concerned only with the question of interceptions effected by or on behalf of the police" - and not other government services such as H.M. Customs and Excise and the Security Service - "within the general context of a criminal investigation, together with the legal and administrative framework relevant to such interceptions".

2. Whether there was any interference with an Article 8 (art. 8) right.

64. It was common ground that one telephone conversation to which the applicant was a party was intercepted at the request of the police under a warrant issued by the Home Secretary (see paragraph 14 above). As telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (art. 8) (see the Klass and Others judgment of 6 September 1978, Series A no. 28, p. 21, para. 41), the admitted measure of interception involved an "interference by a public authority" with the exercise of a right guaranteed to the applicant under paragraph 1 of Article 8 (art. 8-1).

Despite the applicant's allegations, the Government have consistently declined to disclose to what extent, if at all, his telephone calls with mail and telephone interception were liable to be employed. As the Commission pointed out in its report (paragraph 115), the existence in England and Wales of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an "interference ... with the exercise" of the applicant's rights under Article 8 (art. 8), apart from any measures actually taken against him (see the above-mentioned Klass and Others judgment, ibid.). This being so, the Court, like the Commission (see the report, paragraph 114), does not consider it necessary to inquire into the applicant's further claims that both his mail and his telephone calls were intercepted for a number of years.

3. Whether the interferences were justified

65. The principal issue of contention was whether the interferences found were justified under the terms of paragraph 2 of Article 8 (art. 8-2), notably whether they were "in accordance with the law" and "necessary in a democratic society" for one of the purposes enumerated in that paragraph.

(a) "In accordance with the law"

(j) General principles

66. The Court held in its Silver and Others judgment of 25 March 1983 (Series A no. 61, pp. 32-33, para. 85) that, at least as far as interferences with prisoners' correspondence were concerned, the expression "in accordance with the law/ prévue par la loi" in paragraph 2 of Article 8 (art. 8-2) should be interpreted in the light of the same general principles as were stated in the Sunday Times judgment of 26 April 1979 (Series A no. 30) to apply to the comparable expression "prescribed by law/ prévues par la loi" in paragraph 2 of Article 10 (art. 10-2).

The first such principle was that the word "law/loi" is to be interpreted as covering not only written law but also unwritten law (see the above-mentioned Sunday Times judgment, p. 30, para. 47). A second principle, recognised by Commission, Government and applicant as being applicable in the present case, was that "the interference in question must have some basis in domestic law" (see the the above-mentioned Silver and Others judgment, p. 33, para. 86). The expressions in question were, however, also taken to include requirements over and above compliance with the domestic law. Two of these requirements were explained in the following terms:

"Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to
regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.” (Sunday Times judgment, p. 31, para. 49; Silver and Others judgment, p. 33, paras. 87 and 90)

67. In the Government’s submission, these two requirements, which were identified by the Court in cases concerning the imposition of penalties or restrictions on the exercise by the individual of his right to freedom of expression or to correspondence, are less appropriate in the wholly different context of secret surveillance of communications. In the latter context, where the relevant law imposes no restrictions or controls on the individual to which he is obliged to conform, the paramount consideration would appear to the Government to be the lawfulness of the administrative action under domestic law.

The Court would reiterate its opinion that the phrase “in accordance with the law” does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention (see, mutatis mutandis, the above-mentioned Silver and Others judgment, p. 34, para. 90, and the Golder judgment of 21 February 1975, Series A no. 18, p. 17, para. 34). The phrase thus implies - and this follows from the object and purpose of Article 8 (art. 8) - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1) (see the report of the Commission, paragraph 121).

Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident (see the above-mentioned Klass and Others judgment, Series A no. 28, pp. 21 and 23, paras. 42 and 49). Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

68. There was also some debate in the pleadings as to the extent to which, in order for the Convention to be complied with, the “law” itself, as opposed to accompanying administrative practice, should define the circumstances in which and the conditions on which a public authority may interfere with the exercise of the protected rights. The above-mentioned judgment in the case of Silver and Others, which was delivered subsequent to the adoption of the Commission’s report in the present case, goes some way to answering the point. In that judgment, the Court held that "a law which confers a discretion must indicate the scope of that discretion", although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law (ibid., Series A no. 61, pp. 33-34, paras. 88-89). The degree of precision required of the “law” in this connection will depend upon the particular subject-matter (see the above-mentioned Sunday Times judgment, Series A no. 50, p. 31, para. 49). Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

(ii) Application in the present case of the foregoing principles

69. Whilst the exact legal basis of the executive’s power in this respect was the subject of some dispute, it was common ground that the settled practice of intercepting communications, on behalf of the police in pursuance of a warrant issued by the Secretary of State for the purposes of detecting and preventing crime, and hence the admitted interception of one of the applicant's telephone conversations, were lawful under the law of England and Wales. The legality of this power to intercept was established in relation to telephone communications in the judgment of Sir Robert Megarry dismissing the applicant’s civil action (see paragraphs 31-36 above) and, as shown by the independent findings of the Birkett report (see paragraph 28 in fine above), is generally recognised for postal communications.

70. The issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities.

This issue was considered under two heads in the pleadings: firstly, whether the law was such that a communication passing through the services of the Post Office might be intercepted, for police purposes, only pursuant to a valid warrant issued by the Secretary of State and, secondly, to what extent the circumstances in which a warrant might be issued and implemented were themselves circumscribed by law.

71. On the first point, whilst the statements of the established practice given in the Birkett report and the White Paper are categorical para. 55 to the Birkett report and para. 2 of the White Paper - see paragraph 42 above), the law of England and Wales, as the applicant rightly pointed out (see paragraph 56 of the Commission's report), does not expressly make the exercise of the power to intercept communications subject to the issue of a warrant. According to its literal terms, section 80 of the Post Office Act 1969 provides that a "requirement" may be laid on the Post Office to pass information to the police, but it does not in itself render illegal interceptions carried out in the absence of a warrant amounting to a valid "requirement" (see paragraph 29 above). The Commission, however, concluded that this appeared to be the effect of section 80 when read in conjunction with the criminal offences created by section 58 para. 1 of the Post Office Act 1953 and by the other statutory provisions referred to in paragraph 1, subparagraph 1 of Schedule 5 to the 1969 Act (see paragraphs 129-135 of the report, and paragraphs 25, 26 and 30 above).

The reasoning of the Commission was accepted and adopted by the Government but, at least in respect of telephone interceptions, disputed by the applicant. He relied on certain dicta to the contrary in the judgment of Sir Robert Megarry (see paragraphs 31-36 above, especially paragraphs 33 and 35). He also referred to the fact that the 1977 Home Office Consultative Paper, with made notable in the section headed "Supply of information by Post Office to police", of the warrant procedure (see paragraph 50 above).

72. As to the second point, the pleadings revealed a fundamental difference of view as to the effect, if any, of the Post Office Act 1969 in imposing legal restraints on the purposes for which and the manner in which interception of communications may lawfully be authorised by the Secretary of State.

73. According to the Government, the words in section 80 - and, in particular, the phrase "for the like purposes and in the
like manner as, at the passing of this Act, a requirement may be laid - define and restrict the power to intercept by reference to the practice which prevailed in 1968. In the submission of the Government, since the entry into force of the 1969 Act a requirement to intercept communications on behalf of the police can lawfully be imposed on the Post Office only by means of a warrant signed personally by the Secretary of State for the exclusive purpose of the detection of crime and satisfying certain other conditions. Thus, by virtue of section 80 the warrant must, as a matter of law, specify the relevant name, address and telephone number; it must be time-limited and can only be directed to the Post Office, not the police. In addition, the Post Office is only required and empowered under section 80 to make information available to "designated persons holding office under the Crown". Any attempt to broaden or otherwise modify the purposes for which or the manner in which interceptions may be authorised would require an amendment to the 1969 Act which could only be achieved by primary legislation.

74. In its reasoning, which was adopted by the applicant, the Commission drew attention to various factors of uncertainty arguing against the Government's view as to the effect of the 1969 Act (see paragraphs 136-142 of the report).

75. Firstly, the relevant wording of the section, and especially the word "may", appeared to the Commission to authorise the laying of a requirement on the Post Office for whatever purposes and in whatever manner it would previously have been lawfully possible to place a ministerial duty on the Postmaster General, and not to be confined to what actually did happen in practice in 1968. Yet at the time of the Birkett report (see, for example, paragraphs 15, 21, 27, 54-55, 56, 62 and 75) and likewise at the time when the 1969 Act was passed, no clear legal restrictions existed on the permissible "purposes" and "manner". Indeed the Birkett report at one stage (paragraph 62) described the Secretary of State's discretion as "absolute", albeit specifying how its exercise was in practice limited.

76. A further difficulty seen by the Commission is that, on the Government's interpretation, not all the details of the existing arrangements are said to have been incorporated into the law by virtue of section 80 but at least the principal conditions, procedures for the issue of warrants authorising interceptions. Even assuming that the reference to "like purposes" and "like manner" is limited to previous practice as opposed to what would have been legally permissible, it was by no means evident to the Commission what aspects of the previous "purposes" and "manner" have been given statutory basis, so that they cannot be changed save by primary legislation, and what aspects remain matters of administrative discretion susceptible of modification by governmental decision. In this connection, the Commission noted that the notion of "serious crime", which in practice serves as a condition governing when a warrant may be issued for the purpose of the detection of crime, has twice been enlarged since the 1969 Act without recourse to Parliament (see paragraphs 42-43 above).

77. The Commission further pointed out that the Government's analysis of the law was not shared by Sir Robert Megarry in his judgment of February 1979. He apparently accepted the Solicitor General's contentions before him that section 80 referred back to previous administrative arrangements for the issue of warrants (see paragraph 33 above). On the other hand, he plainly considered that these arrangements remained administrative in character and had not, even in their principal aspects, been made binding legal requirements by virtue of section 80 (see paragraph 34 above).

78. It was also somewhat surprising, so the Commission observed, that no mention of section 80 as regulating the issue of warrants should have been made in the White Paper published by the Government in the wake of Sir Robert Megarry's judgment (see paragraph 21 above). Furthermore, the Home Secretary, when presenting the White Paper to Parliament in April 1990, expressed himself in terms suggesting that the existing arrangements as a whole were matters of administrative practice not suitable for being "embodied in legislation", and were subject to change by governmental decision of which Parliament would be informed (see paragraphs 37 in fine and 54 in fine above).

79. The foregoing considerations disclose that, at the very least, in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations. The Court would be usurping the function of the national courts were it to attempt to make an authoritative statement on such issues of domestic law (see, mutatis mutandis, the Deweer judgment of 27 February 1980, Series A no. 35, p. 28, in fine, and the Van Droogenbroeck judgment of 24 June 1982, Series A no. 50, p. 30, fourth sub-paragraph). The Court is, however, required under the Convention to determine whether, for the purposes of paragraph 2 of Article 8 (art. 8-2), the relevant law lays down with reasonable clarity the essential elements of the authorities' powers in this domain. Detailed procedures concerning interception of communications on behalf of the police in England and Wales do exist (see paragraph 62 above), and were subject to change save by primary legislation, and what is more, published statistics show the efficacy of those procedures in keeping the number of warrants granted relatively low, especially when compared with the rising number of indictable crimes committed and telephones installed (see paragraph 53 above). The public have been made aware of the applicable arrangements and principles through publication of the Birkett report and the White Paper and through statements by responsible Ministers in Parliament (see paragraphs 21, 37-38, 41, 43 and 54 above). Nonetheless, on the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect, the Court cannot but reach a similar conclusion to that of the Commission. In the opinion of the Court, the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.

(iii) Conclusion

80. In sum, as far as interception of communications is concerned, the differences with the applicant's right under Article 8 (art. 8) to respect for his private life and correspondence (see paragraph 64 above) were not "in accordance with the law".

(b) "Necessary in a democratic society" for a recognised purpose

81. Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2), (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 23, para. 48). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have
made telephone interception an indispensable tool in the investigation and prevention of serious crime. However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (ibid, p. 26, para. 56). This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse (ibid, p. 23, paras. 49-50).

82. The applicant maintained that the system in England and Wales for the interception of postal and telephone communications on behalf of the police did not meet this condition. In view of its foregoing conclusion that the interferences found were not "in accordance with the law", the Court considers that it does not have to examine further the content of the other guarantees required by paragraph 2 of Article 8 (art. 8-2) and whether the system circumstances.

B. Metering

83. The process known as "metering" involves the use of a device (a meter check printer) which registers the numbers dialled on a particular telephone and the time and duration of each call (see paragraph 56 above). In making such records, the Post Office - now British Telecommunications - makes use only of signals sent to itself as the provider of the telephone service and does not monitor or intercept telephone conversations at all. From this, the Government drew the conclusion that metering, in contrast to interception of communications, does not entail interference with any right guaranteed by Article 8 (art. 8).

84. As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).

85. As was noted in the Commission's decision declaring Mr. Malone's application admissible, his complaints regarding metering are closely connected with his complaints regarding interception of communications. The issue before the Court for decision under this head is similarly limited to the supply of records of metering to the police "within the general context of a criminal investigation, together with the legal and administrative framework relevant [therefor]" (see paragraph 63 above).

86. In England and Wales, although the police do not have any power, in the absence of a subpoena, to compel the production of records of metering, a practice exists whereby the Post Office do on occasions make and provide such records at the request of the police if the information is essential to police enquiries in relation to serious crime and cannot be obtained from other sources (see paragraph 56 above). The applicant, as a suspected receiver of stolen goods, was, it may be presumed, a member of a class of persons potentially liable to be directly affected by this practice. The applicant can therefore claim, for the purposes of Article 25 (art. 25) of the Convention, to be a "victim" of a violation of Article 8 (art. 8) by reason of the very existence of this practice, quite apart from any concrete measure of implementation taken against him (cf, mutatis mutandis, paragraph 64 above). This remains so despite the clarification by the Government that in fact the police had neither caused his telephone to be metered nor undertaken any search operations on the basis of any list of telephone numbers obtained from metering (see paragraph 17 above; see also, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 20, para. 37 in fine).

87. Section 80 of the Post Office Act 1969 has never been applied so as to "require" the Post Office, pursuant to a warrant of the Secretary of State, to make available to the police in connection with the investigation of crime information obtained from metering. On the other hand, no rule of domestic law makes it unlawful for the Post Office voluntarily to comply with a request from the police to make and supply records of metering (see paragraph 56 above). The practice described above, including the limiting conditions as to when the information may be provided, has been made public in answer to parliamentary questions (ibid). However, on the evidence adduced before the Court, apart from the simple absence of prohibition, there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. Consequently, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question was not "in accordance with the law", within the meaning of paragraph 2 of Article 8 (art. 8-2) (see paragraphs 66 to 68 above).

88. This conclusion removes the need for the Court to determine whether the interference found was "necessary in a democratic society" for one of the aims enumerated in paragraph 2 of Article 8 (art. 8-2) (see, mutatis mutandis, paragraph 82 above).

C. Recapitulation

89. There has accordingly been a breach of Article 8 (art. 8) in the applicant's case as regards both interception of communications and release of records of metering to the police.

II. ALLEGED BREACH OF ARTICLE 13 (art. 13)

90. The applicant submitted that no effective domestic remedy existed for the breaches of Article 8 (art. 8) of which he complained and that, consequently, there had also been a violation of Article 13 (art. 13) which provides: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

91. Having regard to its decision on Article 8 (art. 8) (see paragraph 89 above), the Court does not consider it necessary to rule on this issue.

[...]

FOR THESE REASONS, THE COURT

1. Holds unanimously that there has been a breach of Article 8 (art. 8) of the Convention;

2. Holds by sixteen votes to two that it is not necessary also to examine the case under Article 13 (art. 13);

3. Holds unanimously that the question of the application of Article 50 (art. 50) is not ready for decision; accordingly,

(a) reserves the whole of the said question;

(b) refers back to the Chamber the said question.

[...]
CASE OF NIEMIETZ v. GERMANY
(Application no. 13710/88)

JUDGMENT

STRASBOURG
16 December 1992

PROCEDURE

1. The case was referred to the Court by the European Commission of Human Rights ("the Commission") on 12 July 1991, within the three-month period laid down by Article 32 para. 1 and Article 47 (art. 32-1, art. 47) of the Convention. It originated in an application (no. 13710/88) against the Federal Republic of Germany lodged with the Commission under Article 25 (art. 25) on 15 February 1988 by a German citizen, Mr Gottfried Niemietz, who is a lawyer.

[...]

AS TO THE FACTS

I. THE PARTICULAR CIRCUMSTANCES OF THE CASE

6. Mr Niemietz lives in Freiburg im Breisgau, Germany, where he practices as a lawyer (Rechtsanwalt).

7. On 9 December 1985 a letter was sent by telefax from the Freiburg post office to Judge Miosga of the Freising District Court (Amtsgericht). It related to criminal proceedings for insulting behaviour (Beleidigung) pending before that court against Mr J., an employer who refused to deduct from his employees' salaries and pay over to the tax office the Church tax to which they were liable. The letter bore the signature of one Klaus Wegener - possibly a fictitious person -, followed by the words "on behalf of the Anti-clerical Working Group (Antiklerikaler Arbeitskreis) of the Freiburg Bunte Liste (multi-coloured group)" and a post-office box number. It read as follows:

"On 10.12.1985 the trial against Mr [J.] will take place before you. We, the Anti-clerical Working Group of the Freiburg Bunte Liste, protest most strongly about these proceedings. In the FRG, the Church, on the basis of the Hitler concordat and in violation of the State's duty to maintain neutrality, enjoys most extensive privileges. As a result, every non-Christian citizen of this State has to suffer disadvantages and daily annoyance. Among other things, the FRG is the only State which counts the separation of State and Church among its basic principles. This attempt - in a State which counts the separation of State and Church among its basic principles - to insist upon just such a separation has not only exposed [J.] to persistent vexation and interferences on the part of State authorities, culminating in the tax office employing coercive measures, such as attachment, to collect from him Church tax which his employees had already paid a long time previously. It has in addition involved him - when he called these underhand methods by their name - in the present proceedings for alleged insulting behaviour. Were it your task as the competent judge to conduct an unbiased examination of this 'case of insulting behaviour', then it must be said that you have not only failed to carry out this task, but also abused your office in order to try - by means which give a warning and a reminder of the darkest chapters of German legal history - to break the backbone of an unloved opponent of the Church. It was with extreme indignation that we learned of the compulsory psychiatric examination which was conducted on your instructions, and to which [J.] has had to submit in the meantime. We shall use every avenue open to us, in particular our international contacts, to bring to public notice this action of yours, which is incompatible with the principles of a democratic State subscribing to the rule of law. We shall follow the further course of the proceedings against [J.] and expect you to abandon the path of terrorism which you have embarked upon, and to reach the only decision appropriate in this case - an acquittal."  

8. The applicant had, as a city councillor, been chairman for some years of the Freiburg Bunte Liste, which is a local political party. He had also played a particularly committed role in, although he had never been a member of, its Anti-clerical Working Group, which sought to curtail the influence of the Church. Until the end of 1985 certain of the mail for the Bunte Liste, which had as its address for correspondence only the post-office box number that had been given in the letter to Judge Miosga, had been delivered to the office (Bürogemeinschaft) of the applicant and a colleague of his; the latter had also been active on behalf of the party and had acted for it professionally.

9. On 13 January 1986 the Director of the Munich I Regional Court (Landgericht) requested the Munich public prosecutor's office (Staatsanwaltschaft) to institute criminal proceedings against Klaus Wegner for the offence of insulting behaviour, contrary to Article 185 of the Criminal Code. Attempts to serve a summons on him were unsuccessful. The applicant's colleague refused to give any information about Klaus Wegner or his whereabouts and other attempts to identify him failed.

10. In the context of the above-mentioned proceedings the Munich District Court issued, on 8 August 1986, a warrant to search the law office of the applicant and his colleague and the homes of Ms D. and Ms G. The warrant read as follows:

"Preliminary investigations against Klaus Wegner concerning Article 185 of the Criminal Code

Decision

The search of the following residential and business premises for documents which reveal the identity of 'Klaus Wegner' [sic] and the seizure of such documents is ordered.

1. Office premises shared by the lawyers Gottfried Niemietz and [...]
2. Home (including adjoining rooms and cars) of Ms [D.]
3. Home (including adjoining rooms and cars) of Ms [G.]

Reasons

On 9 December 1985 a letter insulting Judge Miosga of the Freising District Court was sent by telefax from the Freiburg post office. It was sent by the Anti-clerical Working Group of the Freiburg Bunte Liste. The letter was signed by one Klaus Wegener. Until now it has not been possible to identify the signatory. The Freiburg Bunte Liste could not be contacted by mail otherwise than through a box number. Until the end of 1985 such mail was forwarded to the office of Niemietz and ..., and since the start of 1986 to Ms [D.]. It has therefore to be assumed that documents throwing light on the identity of Klaus Wegener can be found at the premises of the above-mentioned persons. Furthermore, it is to be assumed that there are such documents in the home of Ms [G.], the Chairwoman of the Freiburg Bunte Liste. For these reasons, it is to be expected that evidence will be found in the course of a search of the premises indicated in this decision.

11. The search of the law office, the need for which the investigating authorities had first tried to obviate by questioning a witness, was effected by representatives of the Freiburg public prosecutor's office and the police on 13 November 1986. According to a police officer's report drawn up on the following day, the premises were entered at about
9.00 a.m. and inspected in the presence of two office assistants. The actual search began at about 9.15 a.m., when the applicant’s colleague arrived, and lasted until about 10.30 a.m. The applicant himself arrived at 9.30 a.m. He declined to give any information as to the identity of Klaus Wegner, on the ground that he might thereby expose himself to the risk of criminal prosecution. Those conducting the search examined four filing cabinets with data concerning clients, three files marked respectively "BL", "C.W. - Freiburg District Court ...", and "G. - Hamburg Regional Court" and three defence files marked respectively "K.W. - Karlsruhe District Court ...", "Niemietz et al. - Freiburg District Court ...", and "D. - Freiburg District Court". According to the applicant, the office’s client index was also looked at and one of the files in question was its "Wegner defence file". Those searching neither found the documents they were seeking nor seized any materials. In the proceedings before the Commission, the applicant stated that he had been able to put aside in time documents pointing to the identity of Klaus Wegner and had subsequently destroyed them.

12. The homes of Ms D. and Ms G. were also searched; documents were found that gave rise to a suspicion that the letter to Judge Miosga had been sent by Ms D. under an assumed name.

13. On 10 December 1986 the Chairman of the Freiburg Bar Association, who had been informed about the search by the applicant’s colleague, addressed a formal protest to the President of the Munich District Court. The Chairman sent copies to the Bavarian Minister of Justice and the Munich Bar Association and invited the latter to associate itself with the protest.

In a reply of 27 January 1987, the President of the Munich District Court stated that the search was proportionate because the letter in question constituted a serious interference with a pending case; hence no legal action on the protest was necessary.

14. The criminal proceedings against "Klaus Wegner" were later discontinued for lack of evidence.

15. On 27 March 1987 the Munich I Regional Court declared an appeal (Beschwerde) lodged by the applicant, pursuant to Article 304 of the Code of Criminal Procedure, against the search warrant to be inadmissible, on the ground that it had already been executed ("wegen prozessueller Überholung"). It considered that in the circumstances there was no legal interest in having the warrant declared unlawful. It had not been arbitrary, since there had been concrete indications that specified material would be found. There was no ground for holding that Article 97 of the Code of Criminal Procedure (see paragraph 21 below) had been circumvented: the warrant had been based on the fact that mail for the Freiburg Bunte Liste had for some time been delivered to the applicant’s office and it could not be assumed that that mail could concern a lawyer-client relationship. In addition, personal honour was not so minor a legal interest as to render the search disproportionate. There could be no question in the present case of preventing a lawyer from freely exercising his profession.

16. On 28 April 1987 the applicant lodged a constitutional complaint (Verfassungsbeschwerde) against the search warrant of 8 August 1986 and the Munich I Regional Court’s decision of 27 March 1987. On 18 August a panel of three judges of the Federal Constitutional Court (Bundesverfassungsgericht) declined to accept the complaint for adjudication, on the ground that it did not offer sufficient prospects of success. The Federal Constitutional Court also found that the Munich I Regional Court’s decision of 27 March 1987 that the applicant’s appeal was inadmissible was not objectionable in terms of constitutional law. Furthermore, as regards the actual execution of the warrant, Mr Niemietz had not exhausted the remedy available to him under section 23(1) of the Introductory Act to the Courts Organisation Act (Einführungsgesetz zum Gerichtsverfassungsgesetz).

II. RELEVANT DOMESTIC LAW

17. The search complained of was ordered in the context of criminal proceedings for insulting behaviour, an offence punishable by imprisonment for a maximum, where no physical violence is involved, of one year or a fine (Article 185 of the Criminal Code).

18. Article 13 para. 1 of the Basic Law (Grundgesetz) guarantees the inviolability of the home (Wohnung); this provision has been consistently interpreted by the German courts in a wide sense, to include business premises (see, in particular, the Federal Constitutional Court’s judgment of 13 October 1971 - Entscheidungs sammlung des Bundesverfassungsgerichts, vol. 52, p. 54).

19. Article 103 of the Code of Criminal Procedure provides that the home and other premises (Wohnung und andere Räume) of a person who is not suspected of a criminal offence may be searched only in order to arrest a person charged with an offence, to investigate indications of an offence or to seize specific objects and provided always that there are facts to suggest that such a person, indications or objects is or are to be found on the premises to be searched.

20. Search warrants may be challenged, as regards their lawfulness, in proceedings instituted under Article 304 of the Code of Criminal Procedure and, as regards their manner of execution, in proceedings instituted under section 23(1) of the Introductory Act to the Courts Organisation Act.

21. In Germany a lawyer is an independent organ in the administration of justice and an independent counsel and representative in all legal matters. An unauthorised breach of secrecy by a lawyer is punishable by imprisonment for a maximum of one year or a fine (Article 203 para. 1(3) of the Criminal Code). A lawyer is entitled to refuse to give testimony concerning any matter confided to him in a professional capacity (Article 53 para. 1(2) and (3) of the Code of Criminal Procedure). The last-mentioned provisions, in conjunction with Article 97, prohibit, with certain exceptions, the seizure of correspondence between lawyer and client.

III. CASE-LAW OF THE COURT OF JUSTICE OF THE EUROPEAN COMMUNITIES

22. In its judgment of 21 September 1989 in Joined Cases 46/87 and 227/88 Hoehst v. Commission [1989] European Court Reports ("ECR") 2859 at 2924, the Court of Justice of the European Communities stated as follows:

"Since the applicant has also relied on the requirements stemming from the fundamental right to the inviolability of the home, it should be observed that, although the existence of such a right must be recognized in the Community legal order as a principle common to the laws of the Member States in regard to the private dwellings of natural persons, the same is not true in regard to undertakings, because there are not inconsiderable divergences between the legal systems of the Member States in regard to the nature and degree of protection afforded to business premises against intervention by the public authorities.

No other inference is to be drawn from Article 8(1) (art. 8-1) of the European Convention on Human Rights which provides that: 'Everyone has the right to respect for his private and family life, his home and his correspondence'. The protective scope of that article is concerned with the development of man’s personal freedom and may not therefore be extended to business premises. Furthermore, it should be noted that there
is no case-law of the European Court of Human Rights on that subject.

None the less, in all the legal systems of the Member States, any intervention by the public authorities in the sphere of private activities of any person, whether natural or legal, must have a legal basis and be justified on the grounds laid down by law, and, consequently, those systems provide, albeit in different forms, protection against arbitrary or disproportionate intervention. The need for such protection must be recognized as a general principle of Community law. In that regard, it should be pointed out that the Court has held that it has the power to determine whether measures of investigation taken by the Commission under the ECSC Treaty are excessive (judgment of 14 December 1962 in Joined Cases 5 to 11 and 13 to 15/62 San Michele and Others v. Commission [1962] ECR 449)." This statement was affirmed in the same court's judgments of 17 October 1989 in Case 85/87 Dow Benelux v. Commission [1989] ECR 3137 at 3157 and Joined Cases 97 to 99/87 Dow Chemical Ibérica and Others v. Commission [1989] ECR 3165 at 3185-6.

[...]

AS TO THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 (art. 8) OF THE CONVENTION

26. Mr Niemietz alleged that the search of his law office had given rise to a breach of Article 8 (art. 8) of the Convention, which reads as follows:

27. In contesting the Commission's conclusion, the Government maintained that Article 8 (art. 8) did not afford protection against the search of a lawyer's office. In their view, the Convention drew a clear distinction between private life and home, on the one hand, and professional and business life and premises, on the other.

28. In arriving at its opinion that there had been an interference with Mr Niemietz's private life and "home", the Commission attached particular significance to the confidential relationship that exists between lawyer and client. The Court shares the Government's doubts as to whether this factor can serve as a workable criterion for the purposes of delimiting the scope of the protection afforded by Article 8 (art. 8). Virtually all professional and business activities may involve, to a greater or lesser degree, matters that are confidential, with the result that, if that criterion were adopted, disputes would frequently arise as to where the line should be drawn.

29. The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly what is an individual's activities "form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.

To deny the protection of Article 8 (art. 8) on the ground that the measure complained of related only to professional activities - as the Government suggested should be done in the present case - could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them. In fact, the Court has not heretofore drawn such distinctions: it concluded that there had been an interference with private life even where telephone tapping covered both business and private calls (see the Huvig v. France judgment of 24 April 1990, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25); and, where a search was directed solely against business activities, it did not rely on that fact as a ground for excluding the applicability of Article 8 (art. 8) under the head of "private life" (see the Chappell v. the United Kingdom judgment of 30 March 1989, Series A no. 152-A, pp. 12-13, para. 26, and pp. 21-22, para. 51).

30. As regards the word "home", appearing in the English text of Article 8 (art. 8), the Court observes that in certain Contracting States, notably Germany (see paragraph 18 above), it has been accepted as extending to business premises. Such an interpretation is, moreover, fully consonant with the French text, since the word "domicile" has a broader connotation than the word "home" and may extend, for example, to a professional person's office.

In this context also, it may not always be possible to draw precise distinctions, since activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises. A narrow interpretation of the words "home" and "domicile" could therefore give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of "private life" (see paragraph 29 above).

31. More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (art. 8), namely to protect the individual against arbitrary interference by the public authorities (see, for example, the Marckx v. Belgium judgment of 13 June 1979, Series A no. 31, p. 15, para. 31). Such an interpretation would not unduly hamper the Contracting States, for they would have to retain their entitlement to "interfere" to the extent permitted by paragraph 2 of Article 8 (art. 8-2); that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case.

32. To the above-mentioned general considerations, which militate against the view that Article 8 (art. 8) is not applicable, must be added a further factor pertaining to the particular circumstances of the case. The warrant issued by the Munich District Court ordered a search for, and seizure of, "documents" - without qualification or limitation - revealing the identity of Klaus Wegner (see paragraph 10 above). Furthermore, those conducting the search examined four cabinets with data concerning clients as well as six individual files (see paragraph 11 above); their operations must perforce have covered "correspondence" and materials that can
properly be regarded as such for the purposes of Article 8 (art. 8). In this connection, it is sufficient to note that that provision does not use, as it does for the word "life", any adjective to qualify the word "correspondence". And, indeed, the Court has already held that, in the context of correspondence in the form of telephone calls, no such qualification is to be made (see the above-mentioned Huvig judgment, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25). Again, in a number of cases relating to correspondence with a lawyer (see, for example, the Schönberger and Durmaz v. Switzerland judgment of 20 June 1988, Series A no. 137, and the Campbell v. the United Kingdom judgment of 25 March 1992, Series A no. 233), the Court did not even advert to the possibility that Article 8 (art. 8) might be inapplicable on the ground that the correspondence was of a professional nature.

33. Taken together, the foregoing reasons lead the Court to find that the search of the applicant's office constituted an interference with his rights under Article 8 (art. 8).

B. Was the interference "in accordance with the law"?

34. The applicant submitted that the interference in question was not "in accordance with the law", since it was based on suspicions rather than facts and so did not meet the conditions laid down by Article 103 of the Code of Criminal Procedure (see paragraph 19 above) and since it was intended to circumvent the legal provisions safeguarding professional secrecy.

35. The Court agrees with the Commission and the Government that that submission must be rejected. It notes that both the Munich I Regional Court and the Federal Constitutional Court considered that the search was lawful in terms of Article 103 of the aforesaid Code (see paragraphs 15-16 and 19 above) and sees no reason to differ from the views which those courts expressed.

C. Did the interference have a legitimate aim or aims?

36. Like the Commission, the Court finds that, as was not contested by the applicant, the interference pursued aims that were legitimate under paragraph 2 of Article 8 (art. 8-2), namely the prevention of crime and the protection of the rights of others, that is the honour of Judge Miosga.

D. Was the interference "necessary in a democratic society"?

37. As to whether the interference was "necessary in a democratic society", the Court inclines to the view that the reasons given therefor by the Munich District Court (see paragraph 10 above) can be regarded as relevant in terms of the legitimate aims pursued. It does not, however, consider it essential to pursue this point since it has formed the opinion that, as was contended by the applicant and as was found by the Commission, the measure complained of was not proportionate to those aims. It is true that the offence in connection with which the search was effected, involving as it did not only an insult to but also an attempt to bring pressure on a judge, cannot be classified as no more than minor. On the other hand, the warrant was drawn in broad terms, in that it ordered a search for and seizure of "documents", without any limitation, revealing the identity of the author of the offensive letter; this point is of special significance where, as in Germany, the search of a lawyer's office is not accompanied by any special procedural safeguards, such as the presence of an independent observer. More importantly, having regard to the materials that were in fact inspected, the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances; it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention. In addition, the attendant publicity must have been capable of affecting adversely the applicant's professional reputation, in the eyes both of his existing clients and of the public at large.

E. Conclusion

38. The Court thus concludes that there was a breach of Article 8 (art. 8).

II. ALLEGED VIOLATION OF ARTICLE 1 OF PROTOCOL No. 1 (P1-1)

39. Mr Niemietz also argued that, by impairing his reputation as a lawyer, the search constituted a violation of Article 1 of Protocol No. 1 (P1-1), which provides:

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

40. Having already taken into consideration, in the context of Article 8 (art. 8), the potential effects of the search on the applicant's professional reputation (see paragraph 37 above), the Court agrees with the Commission that no separate issue arises under Article 1 of Protocol No. 1 (P1-1).

[...]

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. Holds that there has been a violation of Article 8 (art. 8) of the Convention;

2. Holds that no separate issue arises under Article 1 of Protocol No. 1 (P1-1);

3. Dismisses the applicant's claim for just satisfaction.

[...]

311
CASE OF ROTARU v. ROMANIA
(Application no. 28341/95)

JUDGMENT

STRASBOURG

4 May 2000

[...]

PROCEDURE

1. The case was referred to the Court in accordance with the provisions applicable prior to the entry into force of Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by the European Commission of Human Rights ("the Commission") and by a Romanian national, Mr Aurel Rotaru ("the applicant"), on 3 and 29 June 1999 respectively (Article 5 § 4 of Protocol No. 11 and former Articles 47 and 48 of the Convention).

2. The case originated in an application (no. 28341/95) against Romania lodged with the Commission on 22 February 1995 under former Article 25 of the Convention.

The applicant alleged a violation of his right to respect for his private life on account of the holding and use by the Romanian Intelligence Service of a file containing personal information and an infringement of his right of access to a court and his right to a remedy before a national authority that could rule on his application to have the file amended or destroyed.

[...]

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. The applicant's conviction in 1948

7. The applicant, who was born in 1921, was a lawyer by profession. He is now retired and lives in Bârlad.

8. In 1946, after the communist regime had been established, the applicant, who was then a student, was refused permission by the prefect of the county of Vaslui to publish two pamphlets, "Student Soul" (Întrebări de studenți) and "Protests" (Proteste), on the ground that they expressed anti-government sentiments.

9. Dissatisfied with that refusal, the applicant wrote two letters to the prefect in which he protested against the abolition of freedom of expression by the new people's regime. As a result of these letters, the applicant was arrested on 7 July 1948. On 20 September 1948 the Vaslui People's Court convicted the applicant on a charge of insulting behaviour and sentenced him to one year's imprisonment.

B. The proceedings brought under Legislative Decree no. 118/1990

10. In 1989, after the communist regime had been overthrown, the new government caused Legislative Decree no. 118/1990 to be passed, which granted certain rights to those who had been persecuted by the communist regime and who had not engaged in Fascist activities (see paragraph 30 below).

11. On 30 July 1990 the applicant brought proceedings in the Bârlad Court of First Instance against the Ministry of the Interior, the Ministry of Defence and the Vaslui County Employment Department, seeking to have the prison sentence that had been imposed in the 1948 judgment taken into account in the calculation of his length of service at work. He also sought payment of the corresponding retirement entitlements.

12. The court gave judgment on 11 January 1993. Relying on, among other things, the statements of witnesses called by the applicant (P.P. and G.D.), the 1948 judgment and depositions from the University of Iaşi, it noted that between 1946 and 1949 the applicant had been persecuted on political grounds. It consequently allowed his application and awarded him the compensation provided for in Legislative Decree no. 118/1990.

13. As part of its defence in those proceedings, the Ministry of the Interior submitted to the court a letter of 19 December 1990 that it had received from the Romanian Intelligence Service (Serviciul Român de Informaţii – "the RIS"). The letter read as follows:

"In reply to your letter of 11 December 1990, here are the results of our checks on Aurel Rotaru, who lives in Bârlad:
(a) during his studies in the Faculty of Sciences at Iaşi University the aforementioned person was a member of the Christian Students' Association, a 'legionnaire' [legionar]-type[ movement.
(b) in 1946 he applied to the Vaslui censorship office for permission to publish two pamphlets entitled 'Student Soul' and 'Protests' but his request was turned down because of the anti-government sentiments expressed in them;
(c) he belonged to the youth section of the National Peasant Party, as appears from a statement he made in 1948;
(d) he has no criminal record and, contrary to what he maintains, was not imprisoned during the period he mentions;
(e) in 1946-48 he was summoned by the security services on several occasions because of his ideas and questions about his views..."

C. The action for damages against the RIS

14. The applicant brought proceedings against the RIS, stating that he had never been a member of the Romanian legionnaire movement, that he had not been a student in the Faculty of Sciences at Iaşi University but in the Faculty of Law and that some of the other information provided by the RIS in its letter of 19 December 1990 was false and defamatory. Under the Civil Code provisions on liability in tort he claimed damages from the RIS for the non-pecuniary damage he had sustained. He also sought an order, without relying on any particular legal provision, that the RIS should amend or destroy the file containing the information on his supposed legionnaire past.

15. In a judgment of 6 January 1993 the Bucharest Court of First Instance dismissed the applicant's application on the ground that the statutory provisions on tortious liability did not make it possible to allow it.

16. The applicant appealed.

17. On 18 January 1994 the Bucharest County Court found that the information that the applicant had been a legionnaire was false. However, it dismissed the appeal on the ground that the RIS could not be held to have been negligent as it was merely the depositary of the impugned information, and that in the absence of negligence the rules on tortious liability did not apply. The court noted that the information had been gathered by the State's security services, which, when they were disbanded in 1949, had forwarded it to the Securitate (the State Security Department), which had in its turn forwarded it to the RIS in 1990.

18. On 15 December 1994 the Bucharest Court of Appeal dismissed an appeal by the applicant against the judgment of 18 January 1994 in the following terms:

"...the Court finds that the applicant's appeal is ill-founded. As the statutory depositary of the archives of the former State security services, the RIS in its letter no. 70567/1990 forwarded to the Ministry of the Interior information concerning the applicant's activities while he was a university student, as set out by the State security services. It is therefore apparent that
the judicial authorities have no jurisdiction to destroy or amend the information in the letter written by the RIS, which is merely the depositary of the former State security services' archives. In dismissing his application, the judicial authorities did not infringe either Article 1 of the Constitution or Article 3 of the Civil Code but stayed the proceedings in accordance with the jurisdictional rules laid down in the Code of Civil Procedure.”

D. The action for damages against the judges

19. On 13 June 1995 the applicant brought an action for damages against all the judges who had dismissed his application to have the file amended or destroyed. He based his action on Article 3 of the Civil Code, relating to denials of justice, and Article 6 of the Convention. According to the applicant, both the County Court and the Vaslui Court of Appeal refused to register his action.

In this connection, the applicant lodged a fresh application with the Commission on 5 August 1998, which was registered under file no. 46597/98 and is currently pending before the Court.

E. The application for review

20. In June 1997 the Minister of Justice informed the Director of the RIS that the European Commission of Human Rights had declared the applicant's present application admissible. The Minister consequently asked the Director of the RIS to check once again whether the applicant had been a member of the legionnaire movement and, if that information proved to be false, to inform the applicant of the fact so that he could subsequently make use of it in any application for review.

21. On 6 July 1997 the Director of the RIS informed the Minister of Justice that the information in the letter of 19 December 1990 that the applicant had been a legionnaire had been found by consulting their archives, in which a table drawn up by the Iași security office had been discovered that mentioned, in entry 165, one Aurel Rotaru, a “science student, rank-and-file member of the Christian Students' Association, legionnaire”. The Director of the RIS mentioned that the table was dated 15 February 1937 and expressed the view that “since at that date Mr Rotaru was only 16, he could not have been a student in the Faculty of Sciences. [That being so.] we consider that there has been a regrettable mistake which led us to suppose that Mr Aurel Rotaru of Bârlad was the same person as the one who appears in that table as a member of a legionnaire-type organisation. Detailed checks made by our institution in the counties of Iași and Vaslui have not provided any other information to confirm that the two names refer to the same person.”

22. A copy of that letter was sent to the applicant, who on 25 July 1997 applied to the Bucharest Court of Appeal to review its decision of 15 December 1994. In his application he sought a declaration that the defamatory documents were null and void, damages in the amount of one leu in respect of non-pecuniary damage and reimbursement of all the costs and expenses incurred since the beginning of the proceedings, adjusted for inflation.

23. The RIS submitted that the application for review should be dismissed, holding that, in the light of the RIS Director's letter of 6 July 1997, the application had become devoid of purpose.

24. In a final decision of 25 November 1997 the Bucharest Court of Appeal quashed the decision of 15 December 1994 and allowed the applicant’s action, in the following terms: “It appears from letter no. 4173 of 5 July 1997 from the Romanian Intelligence Service . . . that in the archives (shelf-mark 53172, vol. 796, p. 243) there is a table which lists the names of the members of legionnaire organisations who do not live in Iași, entry 165 of which contains the following: 'Rotaru Aurel – science student, rank and-file member of the Christian Students’ Association, legionnaire’. Since the applicant was barely 16 when that table was drawn up, on 15 February 1937, and since he did not attend lectures in the Iași Faculty of Sciences, and since it appears from subsequent checks in the documents listing the names of the members of legionnaire organisations that the name 'Aurel Rotaru' does not seem to be connected with an individual living in Bârlad whose personal details correspond to those of the applicant, the Romanian Intelligence Service considers that a regrettable mistake has been made and that the person mentioned in the table is not the applicant.

Having regard to this letter, the Court holds that it satisfies the requirements of Article 322-5 of the Code of Civil Procedure as it is such as to completely alter the facts previously established. The document contains details which it was not possible to submit at any earlier stage in the proceedings for a reason beyond the applicant's control. That being so, the date on which the Securitate was formed and the way in which the former security services were organised are not relevant factors. Similarly, the fact, albeit a true one, that the Romanian Intelligence Service is only the depositary of the archives of the former security services is irrelevant. What matters is the fact that letter no. 705567 of 19 December 1990 from the Romanian Intelligence Service (Military Unit no. 05007) contains details which do not relate to the applicant, so that the information in that letter is false in respect of him and, if maintained, would seriously injure his dignity and honour.

In the light of the foregoing and in accordance with the aforementioned statutory provision, the application for review is justified and must be allowed. It follows that the earlier decisions in this case must be quashed and that the applicant's action as lodged is allowed.”

25. The court did not make any order as to damages or costs.

II. RELEVANT DOMESTIC LAW

A. The Constitution

26. The relevant provisions of the Constitution read as follows:

Article 20

“(1) The constitutional provisions on citizens’ rights and liberties shall be interpreted and applied in accordance with the Universal Declaration of Human Rights and with the covenants and other treaties to which Romania is a party.

(2) In the event of conflict between the covenants and treaties on fundamental human rights to which Romania is a party and domestic laws, the international instruments shall prevail.”

Article 21

“(1) Anyone may apply to the courts for protection of his rights, liberties and legitimate interests.

(2) The exercise of this right shall not be restricted by any statute.”

B. The Civil Code

27. The relevant provisions of the Civil Code are worded as follows:

Article 3

"A judge who refuses to adjudicate, on the pretext that the law is silent, obscure or defective, may be prosecuted on a charge of denial of justice."

Article 999

"Any act committed by a person who causes damage to another shall render the person through whose fault the damage was caused liable to make reparation for it.”
C. The Code of Civil Procedure

28. The relevant provision of the Code of Civil Procedure reads as follows:
   Article 322-5
   "An application may be made for review of a final decision ... where written evidence which has been withheld by the opposing party or which it was not possible to submit for a reason beyond the parties' control is discovered after the decision has been delivered ..."

D. Decree no. 31 of 1954 on natural and legal persons

29. The relevant provisions of Decree no. 31 of 1954 on natural and legal persons are worded as follows:
   Article 54
   "[1] Anyone whose right ... to honour, reputation ... or any other non-economic right has been infringed may apply to the courts for an injunction prohibiting the act which is infringing the aforementioned rights.
   (2) Similarly, anyone who has been the victim of such an infringement of rights may ask the courts to order the person responsible for the unlawful act to carry out any measure regarded as necessary by the court in order to restore his rights."
   Article 55
   "If a person responsible for unlawful acts does not within the time allowed by the court perform what he has been enjoined to do in order to restore the right infringed, the court may sentence him to pay a periodic pecuniary penalty to the State ..."

E. Legislative Decree no. 118 of 30 March 1990 on the granting of certain rights to persons who were persecuted on political grounds by the dictatorial regime established on 6 March 1945

30. At the material time, the relevant provisions of Legislative Decree no. 118/1990 read:
   Article 1
   "The following periods shall be taken into account in determining seniority and shall count as such for the purpose of calculating retirement pension and any other rights derived from seniority: periods during which a person, after 6 March 1945, for political reasons:
   (a) served a custodial sentence imposed in a final judicial decision or was detained pending trial for political offences;
   (b) joined the Securitate;"
   Article 5
   "A committee composed of a chairman and at most six other members shall be set up in each county ... in order to verify whether the requirements laid down in Article 1 have been satisfied ..." Article 6
   "The chairman must be legally qualified. The committee shall include two representatives from the employment and social-welfare departments and a maximum of four representatives from the association of former political detainees and victims of the dictatorship ..."
   Article 11
   "The provisions of this decree shall not be applicable to persons who have been convicted of crimes against humanity or to those in respect of whom it has been established, by means of the procedure indicated in Articles 5 and 6, that they engaged in Fascist activities within a Fascist-type organisation."

F. Law no. 14 of 24 February 1992 on the organisation and operation of the Romanian Intelligence Service

31. The relevant provisions of Law no. 14 of 24 February 1992 on the organisation and operation of the Romanian Intelligence Service, which was published in the Official Gazette on 3 March 1992, read as follows:
   Section 2
   "The Romanian Intelligence Service shall organise and carry out all activities designed to gather, verify and utilise the information needed for discovering, preventing and frustrating any actions which, in the eyes of the law, threaten Romania's national security."
   Section 8
   "The Romanian Intelligence Service shall be authorised to hold and to make use of any appropriate resources in order to secure, verify, classify and store information affecting national security, as provided by law."
   Article 54
   "All internal documents of the Romanian Intelligence Service shall be secret, shall be kept in its own archives and may be consulted only with the consent of the Director as provided in law. Documents, data and information belonging to the Romanian Intelligence Service shall not be made public until forty years after they have been archived. The Romanian Intelligence Service shall, in order to keep and make use of them, take over all the national-security archives that belonged to the former intelligence services operating on Romanian territory. The national-security archives of the former Securitate shall not be made public until forty years after the date of the passing of this Act."
   G. Law no. 187 of 20 October 1999 on citizens' access to their personal files held on them by the Securitate, enacted with the intention of unmasking that organisation's nature as a political police force.

32. The relevant provisions of Law no. 187 of 20 October 1999, which came into force on 9 December 1999, are worded as follows:
   Section 1
   "[1] All Romanian citizens, and all aliens who have obtained Romanian nationality since 1945, shall be entitled to inspect the files kept on them by the organs of the Securitate ... This right shall be exercisable on request and shall make it possible for the file itself to be inspected and copies to be made of any document in it or relating to its contents.
   (2) Additionally, any person who is the subject of a file from which it appears that he or she was kept under surveillance by the Securitate shall be entitled, on request, to know the identity of the Securitate agents and collaborators who contributed documents to the file.
   (3) Unless otherwise provided by law, the rights provided in subsections (1) and (2) shall be available to the surviving spouses and relatives up to the second degree inclusive of a deceased."
   Section 2
   "[1] In order to provide for a right of access to information of public interest, all Romanian citizens ... the media, political parties ... shall be entitled to be informed ... if any of the persons occupying the following posts or seeking to do so have been agents or collaborators of the Securitate:
   (a) the President of Romania;
   (b) member of Parliament or of the Senate; ..."
   Section 7
   "A National Council for the Study of the Archives of the Securitate [hereinafter 'the Council'], with its headquarters in Bucharest, shall be set up to apply the provisions of this Act. The Council shall be an autonomous body with legal personality, subject to supervision by Parliament. ..."
   Section 8
   "The Council shall consist of a college of eleven members."

314
The members of the college of the Council shall be appointed by Parliament, on a proposal by the parliamentary groups, according to the political composition of the two Chambers — for a term of office of six years, renewable once."

Section 13

"(1) The beneficiaries of this Act may, in accordance with section 1(1), request the Council —
(a) to allow them to consult the files ... compiled by the Securitate up to 22 December 1989;
(b) to issue copies of ... these files ...;
(c) to issue certificates of membership or non-membership of the Securitate and of collaboration or non-collaboration with it;
...

Section 14

"(1) The content of certificates under section 13(1)(c) may be challenged before the college of the Council —

Section 15

"(1) The right of access to information of public interest shall be exercisable by means of a request sent to the Council —

(4) In response to requests made under section 1, the Council shall verify the evidence at its disposal, of whatever form, and shall immediately issue a certificate —

Section 16

"(1) Any beneficiary or person in respect of whom a check has been requested may challenge before the college of the Council a certificate issued under section 15. ...

The college's decision may be challenged — in the Court of Appeal —

THE LAW

I. THE GOVERNMENT'S PRELIMINARY OBJECTIONS

A. Applicant's victim status

33. As their primary submission, the Government maintained — as they had done before the Commission — that the applicant could no longer claim to be the "victim" of a violation of the Convention within the meaning of Article 34. They pointed out that the applicant had won his case in the Bucharest Court of Appeal, since that court had, in its judgment of 25 November 1997, declared null and void the details contained in the letter of 19 December 1990 from the Romanian Intelligence Service (Serviciul Român de Informaţii — "the RIS").

34. The applicant requested the Court to continue its consideration of the case. He argued that the circumstances that had given rise to the application had not fundamentally changed following the decision of 25 November 1997. Firstly, the mere fact of acknowledging, after the Commission's admissibility decision, that a mistake had been made could not amount to adequate redress for the violations of the Convention. Secondly, he had still not had access to his secret file, which was not only stored by the RIS but also used by it. It was consequently not to be excluded that even after the decision of 25 November 1997 the RIS might make use of the information that the applicant had supposedly been a legionnaire and of any other information in his file.

35. The Court reiterates, as to the concept of victim, that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him (see the Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28, pp. 18-19, § 34). Furthermore, "a decision or measure favourable to the applicant is not in principle sufficient to deprive him of his status as a 'victim' unless the national authorities have acknowledged, either expressly or in substance, and then afforded redress for, the breach of the Convention" (see the Amuur v. France judgment of 25 June 1996, Reports of Judgments and Decisions 1996-III, p. 846, § 36, and Daßbauer v. Romania [GC], no. 28114/95, § 44, ECHR 1999-VI).

36. In the instant case the Court notes that the applicant complained of the holding of a secret register containing information about him, whose existence was publicly revealed during judicial proceedings. It considers that he may on that account claim to be the victim of a violation of the Convention. The Court also notes that in a judgment of 25 November 1997 the Bucharest Court of Appeal found that the details given in the letter of 19 December 1990 about the alleged fact that the applicant had been a legionnaire were false, in that they probably related to someone else with the same name, and declared them null and void.

Assuming that it may be considered that that judgment did, to some extent, afford the applicant redress for the existence in his file of information that proved false, the Court takes the view that such redress is only partial and that at all events it is insufficient under the case-law to deprive him of his status of victim. Apart from the foregoing considerations as to his being a victim as a result of the holding of a secret file, the Court points to the following factors in particular. The information that the applicant had supposedly been a legionnaire is apparently still recorded in the RIS's files and no mention of the judgment of 25 November 1997 has been made in the file concerned. Furthermore, the Court of Appeal expressed no view — and was not entitled to do so — on the fact that the RIS was authorised by Romanian legislation to hold and make use of files opened by the former intelligence services, which contained information about the applicant. A key complaint made to the Court by the applicant was that domestic law did not lay down with sufficient precision the manner in which the RIS must carry out its work and that it did not provide citizens with an effective remedy before a national authority.

Lastly, the Bucharest Court of Appeal in its judgment of 25 November 1997 did not rule on the applicant's claim for compensation for non pecuniary damage and for costs and expenses.

37. As to Law no. 187 of 20 October 1999, which the Government relied on, the Court considers, having regard to the circumstances of this case, that it is not relevant (see paragraph 71 below).

38. The Court concludes that the applicant may claim to be a "victim" for the purposes of Article 34 of the Convention. The objection must therefore be dismissed.

B. Exhaustion of domestic remedies

39. The Government also submitted that the application was inadmissible for failure to exhaust domestic remedies. They argued that the applicant had had a remedy which he had not made use of, namely an action based on Decree no. 31/1954 on natural and legal persons, under which the court may order any measure to restrain injury to a person's reputation. The Court notes that there is a close connection between the Government's argument on this point and the merits of the complaints made by the applicant under Article 13 of the Convention. It accordingly joins this objection to the merits (see paragraph 70 below).

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

41. The applicant complained that the RIS held and could at any moment make use of information about his private life,
some of which was false and defamatory. He alleged a violation of Article 8 of the Convention [...]

A. Applicability of Article 8

42. The Government denied that Article 8 was applicable, arguing that the information in the RIS’s letter of 19 December 1990 related not to the applicant’s private life but to his public life. By deciding to engage in political activities and have pamphlets published, the applicant had implicitly waived his right to the “anonymity” inherent in private life. As to his questioning by the police and his criminal record, they were public information.

43. The Court reiterates that the storing of information relating to an individual’s private life in secret register and the release of such information come within the scope of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48).

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of “private life” (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Haffner v. the United Kingdom judgment of 25 June 1997, Reports 1997-III, pp. 1015-16, §§ 42-46).

The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe’s Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is “to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him” (Article 1), such personal data being defined in Article 2 as “any information relating to an identified or identifiable individual” (see Amann v. Switzerland [GC], no. 27798/95, § 6.5, ECHR 2000-II).

Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person’s distant past.

44. In the instant case the Court notes that the RIS’s letter of 19 December 1990 contained various pieces of information about the applicant’s life, in particular his studies, his political activity, his family, his criminal record, some of which had been gathered more than fifty years earlier. In the Court’s opinion, such information, when systematically collected and stored in a file held by the authorities, falls within the scope of “private life” for the purposes of Articles 8 § 1 of the Convention. That is all the more so in the instant case as some of the information has been declared false and is likely to injure the applicant’s reputation.

Article 8 consequently applies.

B. Compliance with Article 8

1. Whether there was interference

45. In the Government’s submission, three conditions had to be satisfied before there could be said to be interference with the right to respect for private life: information had to have been stored about the person concerned; use had to have been made of it; and it had to be impossible for the person concerned to refute it. In the instant case, however, both the storing and the use of the information relating to the applicant had occurred before Romania ratified the Convention. As to the alleged impossibility of refuting the information, the Government maintained that, on the contrary, it was open to the applicant to refute untrue information but that he had not made use of the appropriate remedies.

46. The Court points out that both the storing by a public authority of information relating to an individual’s private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention (see the following judgments: Leander cited above, p. 22, § 48; Kopp v. Switzerland, 25 March 1998, Reports 1998-II, p. 540, § 53; and Amann cited above, §§ 69 and 80). In the instant case it is clear beyond peradventure from the RIS’s letter of 19 December 1990 that the RIS held information about the applicant’s private life. While that letter admittedly predates the Convention’s entry into force in respect of Romania on 20 June 1994, the Government did not submit that the RIS had ceased to hold information about the applicant’s private life after that date. The Court also notes that use was made of some of the information after that date, for example in connection with the application for review which led to the decision of 25 November 1997.

Both the storing of that information and the use of it, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to interference with his right to respect for his private life as guaranteed by Article 8 § 1.

2. Justification for the interference

47. The cardinal issue that arises is whether the interference so found is justified under paragraph 2 of Article 8. That paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be interpreted narrowly. While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as they are necessary for safeguarding the democratic institutions (see the Klass and Others judgment cited above, p. 21, § 42).

48. If it is not to contravene Article 8, such interference must have been “in accordance with the law”, pursue a legitimate aim under paragraph 2 and, furthermore, be necessary in a democratic society in order to achieve that aim.

49. The Government considered that the measures in question were in accordance with the law. The information concerned had been disclosed by the RIS in connection with a procedure provided in Legislative Decree no. 118/1990, which was designed to afford redress to persons persecuted by the communist regime. By the terms of Article 11 of that legislative decree, no measure of redress could be granted to persons who had engaged in Fascist activities.

50. In the applicant’s submission, the keeping and use of the file on him were not in accordance with the law, since domestic law was not sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities were empowered to file information on their private life and make use of it. Furthermore, domestic law did not define with sufficient precision the manner of exercise of those powers and did not contain any safeguards against abuses.

51. The Commission considered that domestic law did not define with sufficient precision the circumstances in which the RIS could archive, release and use information relating to the applicant’s private life.

52. The Court reiterates its settled case-law, according to which the expression “in accordance with the law” not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects (see, as the most recent authority, Amann cited above, § 50).

53. In the instant case the Court notes that Article 6 of Legislative Decree no. 118/1990, which the Government relied on as the basis for the impugned measure, allows any individual to prove that he satisfies the requirements for having certain rights conferred on him, by means of official documents issued by the relevant authorities or other material of evidential value. However, the provision does not lay down the manner in which such evidence may be obtained and does not confer on the RIS any power to gather, store or release information about a person's private life.

The Court must therefore determine whether Law no. 14/1992 on the organisation and operation of the RIS, which was likewise relied on by the Government, can provide the legal basis for these measures. In this connection, it notes that the law in question authorises the RIS to gather, store and use information affecting national security. The Court has doubts as to the relevance to national security of the information held on the applicant. Nevertheless, it reiterates that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law (see the Koppual judgment cited above, p. 541, § 59) and notes that in its judgment of 25 November 1997 the Bucharest Court of Appeal confirmed that it was lawful for the RIS to hold this information as depositary of the archives of the former security services. That being so, the Court may conclude that the storing of information about the applicant's private life had a basis in Romanian law.

54. As to the accessibility of the law, the Court regards that requirement as having been satisfied, seeing that Law no. 14/1992 was published in Romania's Official Gazette on 3 March 1992.

55. As regards the requirement of foreseeability, the Court reiterates that a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct. The Court has stressed the importance of this concept with regard to secret surveillance in the following terms (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, p. 32, § 67, reiterated in Amann cited above, § 56):

"The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the 'quality of the law', requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

56. The "quality" of the legal rules relied on in this case must therefore be scrutinised, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life.

57. The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files. No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law or any other provision does not lay down limits on the age of information held or the length of time for which it may be kept.

Section 45 of the Law empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent. The Court notes that this section contains no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.

58. It also notes that although section 2 of the Law empowers the relevant authorities to permit interferences necessary to prevent and counteract threats to national security, the ground allowing such interferences is not laid down with sufficient precision.

59. The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it (see the Klass and Others judgment cited above, pp. 23-24, §§ 49-50).

In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55).

60. In the instant case the Court notes that the Romanian system for gathering and archiving information does not provide such safeguards, no supervision procedure being provided by Law no. 14/1992, whether while the measure ordered is in force or afterwards.

61. That being so, the Court considers that domestic law does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.

62. The Court concludes that the holding and use by the RIS of information on the applicant's private life were not "in accordance with the law", a fact that suffices to constitute a violation of Article 8. Furthermore, in the instant case that fact prevents the Court from reviewing the legitimacy of the aim pursued by the measures ordered and determining whether they were – assuming the aim to have been legitimate – "necessary in a democratic society".

63. There has consequently been a violation of Article 8.

III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

64. The applicant complained that the lack of any remedy before a national authority that could rule on his application for destruction of the file containing information about him
and amendment of the inaccurate information was also contrary to Article 13, which provides: "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

65. The Government argued that the applicant had obtained satisfaction through the judgment of 25 November 1997, in which the details contained in the RIS's letter of 19 December 1990 had been declared null and void. As to the destruction or amendment of information in the file held by the RIS, the Government considered that the applicant had not chosen the appropriate remedy. He could have brought an action on the basis of Decree no. 31 of 1954, Article 54 § 2 of which empowered the court to order any measure to restore the right infringed, in the instant case the applicant's right to his honour and reputation.

The Government further pointed out that the applicant could now rely on the provisions of Law no. 187 of 1999 to inspect the file opened on him by the Securitate. Under sections 15 and 16 of that Law, the applicant could challenge in court the truth of the information in his file.

66. In the Commission's opinion, the Government had not managed to show that there was in Romanian law a remedy that was effective in practice as well as in law and would have enabled the applicant to complain of a violation of Article 8 of the Convention.

67. The Court reiterates that it has consistently interpreted Article 13 as requiring a remedy in domestic law only in respect of grievances which can be regarded as "arguable" in terms of the Convention (see, for example, Cakici v. Turkey [GC], no. 23657/94, § 112, ECHR 1999-IV). Article 13 guarantees the availability at national level of a remedy to enforce the substance of the Convention rights and freedoms in whatever form they might happen to be secured in the domestic legal order. This Article therefore requires the provision of a domestic remedy allowing the "competent national authority" both to deal with the substance of the relevant Convention complaint and to grant appropriate relief, although Contracting States are afforded some discretion as to the manner in which they conform to their obligation under this provision. The remedy must be "effective" in practice as well as in law (see Wille v. Liechtenstein [GC], no. 28396/95, § 75, ECHR 1999-VII).

68. The Court observes that the applicant's complaint that the RIS held information about his private life for archiving and for use, contrary to Article 8 of the Convention, was indisputably an "arguable" one. He was therefore entitled to an effective domestic remedy within the meaning of Article 13 of the Convention.

69. The "authority" referred to in Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective (see the Klass and Others judgment cited above, p. 30, § 67).

Furthermore, where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual (ibid., p. 31, §§ 70-71).

70. In the instant case the Government maintained that the applicant could have brought an action on the basis of Article 54 of Decree no. 31/1954. In the Court's view, that submission cannot be accepted.

Firstly, it notes that Article 54 of the decree provides for a general action in the courts, designed to protect non-pecuniary rights that have been unlawfully infringed. The Bucharest Court of Appeal, however, indicated in its judgment of 25 November 1997 that the RIS was empowered by domestic law to hold information on the applicant that came from the files of the former intelligence services.

Secondly, the Government did not establish the existence of any domestic decision that had set a precedent in the matter. It has therefore not been shown that such a remedy would have been effective. That being so, this preliminary objection by the Government must be dismissed.

71. As to the machinery provided in Law no. 187/1999, assuming that the Council provided for is set up, the Court notes that neither the provisions relied on by the respondent Government nor any other provisions of that Law make it possible to challenge the holding, by agents of the State, of information on a person's private life or the truth of such information. The supervisory machinery established by sections 15 and 16 relate only to the disclosure of information about the identity of some of the Securitate's collaborators and agents.

72. The Court has not been informed of any other provision of Romanian law that makes it possible to challenge the holding by the intelligence services, of information on the applicant's private life or to refute the truth of such information.

73. The Court consequently concludes that the applicant has been the victim of a violation of Article 13.

IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

74. The applicant complained that the courts' refusal to consider his applications for costs and damages infringed his right to a fair hearing within the meaning of Article 6 § 1. Article 13 provides:

"In the determination of his civil rights and obligations ..., everyone is entitled to a ... hearing ... by [a] ... tribunal..."

75. The Government made no submission.

76. The Commission decided to consider the complaint under the more general obligation, imposed on the States by Article 13, of affording an effective remedy enabling complaints to be made of violations of the Convention.

77. The Court observes that apart from the complaint, examined above, that there was no remedy whereby an application could be made for amendment or destruction of the file containing information about him, the applicant also complained that the Bucharest Court of Appeal, although lawfully seized of a claim for damages and costs, did not rule on the matter in its review judgment of 25 November 1997.

78. There is no doubting that the applicant's claim for compensation for non-pecuniary damage and costs was a civil one within the meaning of Article 6 § 1, and the Bucharest Court of Appeal had jurisdiction to deal with it (see the Robins v. the United Kingdom judgment of 23 September 1997, Reports 1997-V, p. 1809, § 29).

The Court accordingly considers that the Court of Appeal's failure to consider the claim infringed the applicant's right to a fair hearing within the meaning of Article 6 § 1 (see the Ruiz Torija v. Spain judgment of 9 December 1994, Series A no. 303-A, pp. 12-13, § 30).

79. There has therefore been a violation of Article 6 § 1 of the Convention also.

[...]

FOR THESE REASONS, THE COURT

1. Dismisses unanimously the Government's preliminary objection that the applicant was no longer a victim;
2. Joins to the merits unanimously the Government’s preliminary objection of failure to exhaust domestic remedies and dismisses it unanimously after consideration of the merits;

3. Holds by sixteen votes to one that there has been a violation of Article 8 of the Convention;

4. Holds unanimously that there has been a violation of Article 13 of the Convention;

5. Holds unanimously that there has been a violation of Article 6 § 1 of the Convention;

6. Holds unanimously:
   (a) that the respondent State is to pay the applicant, within three months, FRF 50,000 (fifty thousand French francs) in respect of non pecuniary damage and FRF 13,450 (thirteen thousand four hundred and fifty French francs) for costs and expenses, less FRF 9,759.72 (nine thousand seven hundred and fifty-nine French francs seventy-two centimes) to be converted into Romanian lei at the rate applicable at the date of settlement;
   (b) that simple interest at an annual rate of 2.74% shall be payable from the expiry of the above-mentioned three months until settlement;

7. Dismisses unanimously the remainder of the applicant’s claim for just satisfaction.

[...]

COPLAND v. THE UNITED KINGDOM
(Application no. 62617/00)

JUDGMENT

STRASBOURG

3 April 2007

[...]

PROCEDURE

1. The case originated in an application (no. 62617/00) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Ms Lynette Copland ("the applicant")

2. The applicant complained about the monitoring of her telephone calls, e-mail correspondence and internet usage under Articles 8 and 13.

[...]

THE FACTS

1. THE CIRCUMSTANCES OF THE CASE

6. The applicant was born in 1950 and lives in Llanelli, Wales.

7. In 1991 the applicant was employed by Carmarthenshire College ("the College"). The College is a statutory body administered by the State and possessing powers under sections 18 and 19 of the Further and Higher Education Act 1992 relating to the provision of further and higher education.

8. In 1995 the applicant became the personal assistant to the College Principal ("CP") and from the end of 1995 she was required to work closely with the newly appointed Deputy Principal ("DP").

9. In about July 1998, whilst on annual leave, the applicant visited another campus of the College with a male director. She subsequently became aware that the DP had contacted that campus to enquire about her visit and understood that he was suggesting an improper relationship between her and the director.

10. During her employment, the applicant’s telephone, e-mail and internet usage were subjected to monitoring at the DP’s instigation. According to the Government, this monitoring took place in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes. The Government stated that the monitoring of telephone usage consisted of analysis of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost. The applicant also believed that there had been detailed and comprehensive logging of the length of calls, the number of calls received and made and the telephone numbers of individuals calling her. She stated that on at least one occasion the DP became aware of the name of an individual with whom she had exchanged incoming and outgoing telephone calls. The Government submitted that the monitoring of telephone usage took place for a few months up to about 22 November 1999. The applicant contended that her telephone usage was monitored over a period of about 18 months until November 1999.

11. The applicant’s internet usage was also monitored by the DP. The Government accepted that this monitoring took the form of analysing the web sites visited, the times and dates of the visits to the web sites and their duration and that this monitoring took place from October to November 1999. The applicant did not comment on the manner in which her internet usage was monitored but submitted that it took place over a much longer period of time than the Government admit.

12. In November 1999 the applicant became aware that enquiries were being made into her use of e-mail at work when her step-daughter was contacted by the College and asked to supply information about e-mails that she had sent to the College. The applicant wrote to the CP to ask whether there was a general investigation taking place or whether her e-mails only were being investigated. By an e-mail dated 24 November 1999 the CP advised the applicant that, whilst all e-mail activity was logged, the information department of the College was investigating only her e-mails, following a request by the DP.

13. The Government submitted that monitoring of e-mails took the form of analysis of e-mail addresses and dates and times at which e-mails were sent and that the monitoring occurred for a few months prior to 22 November 1999. According to the applicant the monitoring of e-mails occurred for at least six months from May 1999 to November 1999. She provided documentary evidence in the form of printouts detailing her e-mail usage from 14 May 1999 to 22 November 1999 which set out the date and time of e-mails sent from her e-mail account together with the recipients e-mail addresses.

14. By a memorandum dated 29 November 1999 the CP wrote to the DP to confirm the contents of a conversation they had had in the following terms:

"To avoid ambiguity I felt it worthwhile to confirm my views expressed to you last week, regarding the investigation of [the applicant’s] e-mail traffic.

Subsequent to [the applicant] becoming aware that someone from [the College] had been following up her e-mails, I spoke to [ST] who confirmed that this was true and had been instigated by yourself. Given the forthcoming legislation making it illegal for organisations to examine someone’s e-mail without permission, I naturally felt concerned over recent events and instructed [ST] not to carry out any further analysis. Furthermore, I asked you to do likewise and asked that any information you have of concern regarding [the applicant] be forwarded to me as a matter of priority. You indicated that you would respond positively to both requests, whilst re-affirming your concerns regarding [the applicant]."
15. There was no policy in force at the College at the material time regarding the monitoring of telephone, e-mail or internet use by employees.

16. In about March or April 2000 the applicant was informed by other members of staff at the College that between 1996 and late 1999 several of her activities had been monitored by the DP or those acting on his behalf. She further believed that the DP became aware of a legally privileged fax that was sent by herself to her solicitors and that her personal movements, both at work and when on annual or sick leave, were the subject of surveillance.

17. The applicant provided the Court with statements from other members of staff alleging inappropriate and intrusive monitoring of their movements. The applicant, who is still employed by the College, understands that the DP has been suspended.

II. RELEVANT DOMESTIC LAW

A. Law of privacy

18. At the relevant time there was no general right to privacy in English law.

19. Since the implementation of the Human Rights Act 1998 on 2 October 2000, the courts have been required to read and give effect to primary legislation in a manner which is compatible with Convention rights so far as possible. The Act also made it unlawful for any public authority, including a court, to act in a manner which is incompatible with a Convention right unless required to do so by primary legislation, thus providing for the development of the common law in accordance with Convention rights. In the case of Douglas v Hello! Ltd ([2001] 1 WLR 992), Sedley LJ indicated that he was prepared to find that there was a qualified right to privacy under English law, but the Court of Appeal did not rule on the point.

20. The Regulation of Investigatory Powers Act 2000 (‘the 2000 Act’) provided for the regulation of, inter alia, interception of communications. The Telecommunications (Lawful Business Practice) Regulations 2000 were promulgated under the 2000 Act and came into force on 24 October 2000. The Regulations set out the circumstances in which employers could record or monitor employees’ communications (such as e-mail or telephone) without the consent of either the employee or the other party to the communication. Employers were required to take reasonable steps to inform employees that their communications might be intercepted.

B. Contractual damages for breach of trust and confidence by employer

21. The House of Lords in Malik v Bank of Credit and Commerce International SA [1997] IRLR 462 confirmed that, as a matter of law, a general term is implied into each employment contract that an employer will not “without reasonable and proper cause, conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between employer and employee”. In Malik, the House of Lords was concerned with the award of so-called “stigma compensation” where an ex-employee is unable to find further employment due to association with a dishonest former employer. In considering the damages that could be awarded for breach of the obligation of trust and confidence, the House were solely concerned with the payment of compensation for financial loss resulting from handicap in the labour market. Lord Nicholls expressly noted that, “[f]or the present purposes I am not concerned with the exclusion of damages for injured feelings, the present case is concerned only with financial loss.”

22. In limiting the scope of the implied term of trust and confidence in Malik, Lord Steyn stated as follows: “the implied mutual obligation of trust and confidence applies only where there is ‘no reasonable and proper cause’ for the employer’s conduct, and then only if the conduct is calculated to destroy or seriously damage the relationship of trust and confidence. That circumscribes the potential reach and scope of the implied obligation.”

C. Tort of misfeasance in public office

23. The tort of misfeasance in public office arises when a public official has either (a) exercised his power specifically intending to injure the plaintiff, or (b) acted in the knowledge of, or with reckless indifference to, the illegality of his act and in the knowledge or with reckless indifference to the probability of causing injury to the claimant or a class of people of which the claimant is a member (Three Rivers D.C. v. Bank of England (N0.3) [HL] [2000] WLR 1220).

D. Data Protection Act 1984

24. At the time of the acts complained of by the applicant, the Data Protection Act 1984 (‘the 1984 Act’) regulated the manner in which people and organisations that held data, known as “data holders”, processed or used that data. It provided certain actionable remedies to individuals in the event of misuse of their personal data. The 1984 Act has now been replaced by the Data Protection Act 1998.

25. Section 1 of the 1984 Act defined its terms as follows: “(2) ‘Data’ means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose.

3. ‘Personal data’ means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user...)

4. ‘Data subject’ means an individual who is the subject of personal data.

5. ‘Data user’ means a person who holds data, and a person ‘holds’ data if –

(a) the data form part of a collection of data processed or intended to be processed by or on behalf of that person as mentioned in subsection (2) above; and

(b) that person... controls the contents and use of the data comprised in the collection; and

(c) the data are in the form in which they have been or are intended to be processed as mentioned in paragraph (a)...”

7. ‘Processing’ in relation to data means amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of these operations by reference to the data subject.

9. ‘Disclosing’ in relation to data, includes disclosing information extracted from the data...”

26. The “data protection principles” to be respected by data holders were set out in Part 1 to Schedule 1 of the Act as follows:

“1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

2. Personal data shall be held only for one or more specified and lawful purposes...

4. Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose or those purposes.”
27. Section 23 of the 1984 Act provided rights to compensation for the data subject in the event of unauthorised disclosure of personal data:

"(1) An individual who is the subject of personal data held by a data user...and who suffers damage by reason of -

(2) The disclosure of the data or, access having been obtained to the data, without such authority as aforesaid, shall be entitled to compensation from the data user...for that damage and for any distress which the individual has suffered by reason of the disclosure or access."

28. The 1984 Act also created the position of Data Protection Registrar, under a duty to promote the observance of the data protection principles by data users. In section 10 it created a criminal offence as follows:

"(1) If the Registrar is satisfied that a registered person has contravened or is contravening any of the data protection principles he may serve him with a notice (an enforcement notice) requiring him to take - such steps as are so specified for complying with the principle or principles in question.

(2) In deciding whether to serve an enforcement notice, the Registrar shall consider whether the contravention has caused or is likely to cause any person damage or distress.

(9) Any person who fails to comply with an enforcement notice shall be guilty of an offence..."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

29. The applicant alleged that the monitoring activity that took place amounted to an interference with her right to respect for private life and correspondence under Article 8 ( [...].

30. The Government contested that argument.

A. The parties' submissions

1. The Government

31. The Government accepted that the College was a public body for whose actions the State was directly responsible under the Convention.

32. Although there had been some monitoring of the applicant's telephone calls, e-mails and internet usage prior to November 1999, this did not extend to the interception of telephone calls or the analysis of the content of websites visited by her. The monitoring thus amounted to nothing more than the analysis of automatically generated information to determine whether College facilities had been used for personal purposes which, of itself, did not constitute a failure to respect private life or correspondence. The case of P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001 IX, could be distinguished since there actual interception of telephone calls occurred. There were significant differences from the case of Halford v. the United Kingdom, judgment of 25 June 1997, Reports of Judgments and Decisions 1997 III, where the applicant's telephone calls were intercepted on a telephone which had been designated for private use and, in particular, her litigation against her employer.

33. In the event that the analysis of records of telephone, e-mail and internet usage was considered to amount to an interference with respect for private life or correspondence, the Government contended that the interference was justified.

34. First, it pursued the legitimate aim of protecting the rights and freedoms of others by ensuring that the facilities provided by a publicly funded employer were not abused. Secondly, the interference had a basis in domestic law in that the College, as a statutory body, whose powers enable it to provide further and higher education and to do anything necessary and expedient for those purposes, had the power to take reasonable control of its facilities to ensure that it was able to carry out its statutory functions. It was reasonably foreseeable that the facilities provided by a statutory body out of public funds could not be used excessively for personal purposes and that the College would undertake an analysis of its records to determine if there was any likelihood of personal use which needed to be investigated. In this respect, the situation was analogous to that in Peck v. the United Kingdom, no. 44647/98, ECHR 2003 I.

35. Finally, the acts had been necessary in a democratic society and were proportionate as any interference went no further than necessary to establish whether there had been such excessive personal use of facilities as to merit investigation.

2. The applicant

36. The applicant did not accept that her e-mails were not read and that her telephone calls were not intercepted but contended that, even if the facts were as set out by the Government, it was evident that some monitoring activity took place amounting to an interference with her right to respect for private life and correspondence.

[...]

38. The applicant asserted that the conduct of the College was neither necessary nor proportionate. There were reasonable and less intrusive methods that the College could have used such as drafting and publishing a policy dealing with the monitoring of employees' usage of the telephone, internet and e-mail.

B. The Court's assessment

39. The Court notes the Government's acceptance that the College is a public body for whose acts it is responsible for the purposes of the Convention. Thus, it considers that in the present case the question to be analysed under Article 8 relates to the negative obligation on the State not to interfere with the private life and correspondence of the applicant and that no separate issue arises in relation to home or family life.

40. The Court further observes that the parties disagree as to the nature of this monitoring and the period of time over which it took place. However, the Court does not consider it necessary to enter into this dispute as an issue arises under Article 8 even on the facts as admitted by the Government.

1. Scope of private life

41. According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8 § 1 (see Halford, cited above, § 44 and Amann v. Switzerland [GC], no. 27798/95, § 43, ECHR 2000 II). It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage.

42. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford, § 45). The same expectation should apply in relation to the applicant's e-mail and internet usage.

2. Whether there was any interference with the rights guaranteed under Article 8.

43. The Court observes that the use of information relating to the date and length of telephone conversations and in
particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone" (see Malone v. the United Kingdom, judgment of 2 August 1984, Series A no. 82, § 94). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1 (see Amann, cited above, § 65). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.

44. Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.

3. Whether the interference was “in accordance with the law”

45. The Court recalls that it is well established in the case-law that the term "in accordance with the law" implies - and this follows from the object and purpose of Article 8 - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8 § 1. This is all the more so in areas such as the monitoring in question, in view of the lack of public scrutiny and the risk of misuse of power (see Halford, cited above, § 49).

46. This expression not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law (see, inter alia, Khan v. the United Kingdom, judgment of 12 May 2000, Reports of Judgments and Decisions 2000-V, § 26; P.G. and J.H. v. the United Kingdom, cited above, § 44). In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures (see Halford, cited above, § 49 and Malone, cited above, § 67).

47. The Court is not convinced by the Government’s submission that the College was authorised under its statutory powers to do “anything necessary or expedient” for the purposes of providing higher and further education, and finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the internet by employees. Furthermore, it is clear that the Telecommunications (Lawful Business Practice) Regulations 2000 (adopted under the Regulation of Investigatory Powers Act 2000) which make such provision were not in force at the relevant time.

48. Accordingly, as there was no domestic law regulating monitoring at the relevant time, the interference in this case was not “in accordance with the law” as required by Article 8 § 2 of the Convention. The Court would not exclude that the monitoring of an employee’s use of a telephone, e-mail or internet at the place of work may be considered “necessary in a democratic society” in certain situations in pursuit of a legitimate aim. However, having regard to its above conclusion, it is not necessary to pronounce on that matter in the instant case.

49. There has therefore been a violation of Article 8 in this regard.

II. ALLEGED VIOLATION OF ARTICLE 13 IN CONJUNCTION WITH ARTICLE 8 OF THE CONVENTION

50. The applicant submitted that no effective domestic remedy existed for the breaches of Article 8 of which she complained and that, consequently, there had also been a violation of Article 13 which provides as follows: “Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.”

51. Having regard to its decision on Article 8 (see paragraph 48 above), the Court does not consider it necessary to examine the applicant’s complaint also under Article 13.

[...]

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. Holds that there has been a violation of Article 8 of the Convention;

2. Holds that it is not necessary to examine the case under Article 13 of the Convention.

[...]
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),
Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate the facilitated exchange of personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in

...
Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection
shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable of being used or decisions regarding any particular individual;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with Freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing
operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(29) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;
(53) Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (4);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular
as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive’s provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State’s regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1 Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2 Definitions

For the purposes of this Directive:

(a) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’): an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) ‘personal data filing system’ (‘filing system’) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) ‘controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) ‘third party’ shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) ‘recipient’ shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) ‘the data subject’s consent’ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to the processing of personal data relating to him being processed.

Article 3 Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

— by a natural person in the course of a purely personal or household activity.

Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the
territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:
   (a) processed fairly and lawfully;
   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:
   (a) the data subject has unambiguously given his consent; or
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
   (d) processing is necessary in order to protect the vital interests of the data subject; or
   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:
   (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
   (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
   (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
   (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
   (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary
expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
   — the recipients or categories of recipients of the data,
   — whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
   — the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
   — the categories of data concerned,
   — the recipients or categories of recipients,
   — the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:
   — confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
   — communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
   — knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 [1];
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 13 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.
Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

**Article 15**

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

   (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
   
   (b) is authorized by a law which also lays down measures to safeguard the data subject’s legitimate interests.

**SECTION VIII**

CONFIDENTIALITY AND SECURITY OF PROCESSING

**Article 16**

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

**Article 17**

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The controller shall act only on instructions from the controller, and stating in particular that:

   — the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

**SECTION IX**

NOTIFICATION

**Article 18**

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for a simplification of or exemption from notification only in the following cases and under the following conditions:

   — where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
   
   — where the controller, in compliance with the national law which governs him, appoints a personal data protection official responsible in particular:

      — for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

      — for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2).

   thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

**Article 19**

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

   (a) the name and address of the controller and of his representative, if any;
   
   (b) the purpose or purposes of the processing;
   
   (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
   
   (d) the recipients or categories of recipient to whom the data might be disclosed;
   
   (e) proposed transfers of data to third countries;
   
   (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.
Article 20
Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21
Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.
2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.
   The register shall contain at least the information listed in Article 19 (1) (a) to (e).
   The register may be inspected by any person.
3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e).
   Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III
JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22
Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23
Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24
Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25
Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
   Member States shall take the measures necessary to comply with the Commission's decision.

Article 26
Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
   (a) the data subject has given his consent unambiguously to the proposed transfer; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adds adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary measures to comply with the Commission’s decision.
4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission’s decision.

CHAPTER V
CODES OF CONDUCT

Article 27
1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI
SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28
Supervisory authority
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them.
2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.
3. Each authority shall in particular be endowed with:
— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
the power to engage in legal proceedings, where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.
Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.
5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.
6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.
7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29
Working Party on the Protection of Individuals with regard to the Processing of Personal Data
1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as ‘the Working Party’, is hereby set up. It shall have advisory status and act independently.
2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. Each member of the Working Party shall be designated by the institution, authority or authorities which he represents.
Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman’s term of office shall be two years. His appointment shall be renewable.

5. The Working Party’s secretariat shall be provided by the Commission.


7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission’s request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party’s opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption. When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),
Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where
this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the Directive on electronic communications services and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject’s consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and to visit information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of
communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to track the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail, the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of the unauthorised use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they
should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or
cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail’s content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (4) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope and aim

1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/29/EC of the European Parliament and of the Council of 7 March 2002 on a common
regulatory framework for electronic communications networks and services (Framework Directive) (8) shall apply. The following definitions shall also apply:

(a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) 'location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

(i) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Article 3
Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

Article 4
Security of processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and

— ensure the implementation of a security policy with respect to the processing of personal data,

1a. Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

3. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

3. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

3. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

3. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

4. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

5. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).
Article 5
Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Article 6
Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.
2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber’s terminal.

Article 12

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.

Article 14

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the
Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications (10).

Article 14a
Committee procedure

1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

Article 15
Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

1b. Providers shall establish internal procedures for responding to requests for access to users’ personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 15a
Implementation and enforcement

1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.

2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.

4. The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission’s comments or recommendations when deciding on the measures.

Article 16
Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17
Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.
2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18
Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. [...] 

Article 19
Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1). References made to the repealed Directive shall be construed as being made to this Directive.

Article 20
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

[...]


Amended by:

Official Journal

<table>
<thead>
<tr>
<th>No</th>
<th>page</th>
<th>date</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>54</td>
<td>13.4.2006</td>
</tr>
<tr>
<td>M2</td>
<td>11</td>
<td>18.12.2009</td>
</tr>
</tbody>
</table>


Relevant Case Law on the Directives 95/46/EC; 2002/58/EC

Case C-101/01 Criminal proceedings against Bodil Lindqvist

 [...] 

The main proceedings and the questions referred

 [...] 

(1) Is the mention of a person — by name or with name and telephone number — on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute the processing of personal data wholly or partly by automatic means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?

(2) If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)?

If the answer to either of those questions is yes, the hovrätt also asks the following questions:

(3) Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?

(4) Is information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?

(5) [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden — with the result that personal data become accessible to people in third countries — does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?

(6) Can the provisions of [Directive 95/46], in a case such as the above, be regarded as bringing about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms?

Finally, the hovrätt asks the following question:

(7) Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the directive, even if none of the circumstances described in Article 13 exists?

[...] 

On those grounds,

THE COURT,

in answer to the questions referred to it by the Göta hovrätt by order of 23 February 2001, hereby rules:

1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2. Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

3. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

4. There is no transfer of data to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

5. The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.

6. Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

[...]
Does Community law, specifically Articles 15(2) and 18 of Directive [2000/31], Article 8(1) and (2) of Directive [2001/29], Article 8 of Directive [2004/48] and Articles 17(2) and 47 of the Charter ... permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service? 

On those grounds, the Court (Grand Chamber) hereby rules:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

Is the term "intermediary" in Article 5(1)(a) and Article 8(3) of Directive [2001/29] to be interpreted as including an access provider who merely provides a user with access to the network by allocating him a dynamic IP address but does not himself provide him with any services such as email, FTP or file-sharing services and does not exercise any control, whether de iure or de facto, over the services which the user makes use of?

If the first question is answered in the affirmative:

Is Article 8(3) of Directive [2004/48], regard being had to Article 6 and Article 15 of Directive [2002/58], to be interpreted (restrictively) as not permitting the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright (rights of exploitation and use)?

On those grounds, the Court (Eighth Chamber) hereby rules:


2. Access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether de iure or de facto, over the services which users make use of, must be regarded as ‘intermediaries’ within the meaning of Article 8(3) of Directive 2001/29.

‘1. Does Directive [2006/24], and in particular Articles 3 to 5 and 11 thereof, preclude the application of a national provision which is based on Article 8 of [Directive 2004/48] and which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which address is claimed, was used in the infringement? The question is based on the assumption that the applicant has adduced clear evidence of the infringement of a particular copyright and that the measure is proportionate.

2. Is the answer to Question 1 affected by the fact that the Member State has not implemented [Directive 2006/24] despite the fact that the period prescribed for implementation has expired?’
On those grounds, the Court (Third Chamber) hereby rules:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC must be interpreted as not precluding the application of national legislation based on Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights which, in order to identify an internet subscriber or user, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement, since that legislation does not fall within the material scope of Directive 2006/24.

It is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired.

Directives 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings insofar as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

[...]

Joined Cases C-293/12 and C-594/12, (Digital Rights Ireland Ltd, Kärntner Landesregierung)

[...]

Case C-293/12

[...]

‘1. Is the restriction on the rights of the [plaintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 — and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime? and/or

b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]administration laid down in Article 41 of the Charter?’

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof [as informed by Article 8 of the ECHR]?

Case C-594/12

[...]

1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/24] and Regulation … No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?’

[...]

On those grounds, the Court (Grand Chamber) hereby rules:


Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,

1. Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the
protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).

2. Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

3. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

4. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů,

[...]

18. In those circumstances, the Nejvyšší správní soud decided to stay proceedings and refer the following question to the Court of Justice for a preliminary ruling:

‘Can the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home be classified as the processing of personal data “by a natural person in the course of a purely personal or household activity” for the purposes of Article 3(2) of Directive 95/46 ... even though such a system also monitors a public space?’

On those grounds, the Court (Fourth Chamber) hereby rules:

The second indent of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision...
X. E-Finance

Treaty on the functioning of the European Union (relevant provisions on free movement of persons, services and capital, euro currency and European Central Bank connected with E-Finance)

[...]}

TITLE IV FREE MOVEMENT OF PERSONS, SERVICES AND CAPITAL

CHAPTER 2
RIGHT OF ESTABLISHMENT

Article 49
Within the framework of the provisions set out below, restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State shall be prohibited. Such prohibition shall also apply to restrictions on the setting-up of agencies, branches or subsidiaries by nationals of any Member State established in the territory of any Member State.

Freedom of establishment shall include the right to take up and pursue activities as self-employed persons and to set up and manage undertakings, in particular companies or firms within the meaning of the second paragraph of Article 54, under the conditions laid down for its own nationals by the law of the country where such establishment is effected, subject to the provisions of the Chapter relating to capital.

[...]

Article 54
Companies or firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Union shall, for the purposes of this Chapter, be treated in the same way as natural persons who are nationals of Member States. ‘Companies or firms’ means companies or firms constituted under civil or commercial law, including cooperative societies, and other legal persons governed by public or private law, save for those which are non-profit-making.

Article 55
Member States shall accord nationals of the other Member States the same treatment as their own nationals as regards participation in the capital of companies or firms within the meaning of Article 54, without prejudice to the application of the other provisions of the Treaties.

[...]

CHAPTER 3
SERVICES

Article 57
Services shall be considered to be ‘services’ within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons. ‘Services’ shall in particular include:
(a) activities of an industrial character;
(b) activities of a commercial character;
(c) activities of craftsmen;
(d) activities of the professions.

Without prejudice to the provisions of the Chapter relating to the right of establishment, the person providing a service may, in order to do so, temporarily pursue his activity in the Member State where the service is provided, under the same conditions as are imposed by that State on its own nationals.

Article 58
[...]

2. The liberalisation of banking and insurance services connected with movements of capital shall be effected in step with the liberalisation of movement of capital.

[...]

Article 61
As long as restrictions on freedom to provide services have not been abolished, each Member State shall apply such restrictions without distinction on grounds of nationality or residence to all persons providing services within the meaning of the first paragraph of Article 56.

[...]

CHAPTER 4
CAPITAL AND PAYMENTS

Article 63
1. Within the framework of the provisions set out in this Chapter, all restrictions on the movement of capital between Member States and between Member States and third countries shall be prohibited.

2. Within the framework of the provisions set out in this Chapter, all restrictions on payments between Member States and between Member States and third countries shall be prohibited.

Article 64
1. The provisions of Article 63 shall be without prejudice to the application to third countries of any restrictions which exist on 31 December 1993 under national or Union law adopted in respect of the movement of capital to or from third
countries involving direct investment — including in real estate — establishment, the provision of financial services or the admission of securities to capital markets. In respect of restrictions existing under national law in Bulgaria, Estonia and Hungary, the relevant date shall be 31 December 1999.

2. Whilst endeavouring to achieve the objective of free movement of capital between Member States and third countries to the greatest extent possible and without prejudice to the other Chapters of the Treaties, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt the measures on the movement of capital to or from third countries involving direct investment — including investment in real estate — establishment, the provision of financial services or the admission of securities to capital markets.

3. Notwithstanding paragraph 2, only the Council, acting in accordance with a special legislative procedure, may unanimously, and after consulting the European Parliament, adopt measures which constitute a step backwards in Union law as regards the liberalisation of the movement of capital to or from third countries.

Article 65
1. The provisions of Article 63 shall be without prejudice to the right of Member States:

(a) to apply the relevant provisions of their tax law which distinguish between taxpayers who are not in the same situation with regard to their place of residence or with regard to the place where their capital is invested;

(b) to take all requisite measures to prevent infringements of national law and regulations, in particular in the field of taxation and the prudential supervision of financial institutions, or to lay down procedures for the declaration of capital movements for purposes of administrative or statistical information, or to take measures which are justified on grounds of public policy or public security.

2. The provisions of this Chapter shall be without prejudice to the applicability of restrictions on the right of establishment which are compatible with the Treaties.

3. The measures and procedures referred to in paragraphs 1 and 2 shall not constitute a means of arbitrary discrimination or a disguised restriction on the free movement of capital and payments as defined in Article 63.

4. In the absence of measures pursuant to Article 64(3), the Commission or, in the absence of a Commission decision within three months from the request of the Member State concerned, the Council, may adopt a decision stating that restrictive tax measures adopted by a Member State concerning one or more third countries are to be considered compatible with the Treaties in so far as they are justified by one of the objectives of the Union and compatible with the proper functioning of the internal market. The Council shall act unanimously on application by a Member State.

Article 66
Where, in exceptional circumstances, movements of capital to or from third countries cause, or threaten to cause, serious difficulties for the operation of economic and monetary union, the Council, on a proposal from the Commission and after consulting the European Central Bank, may take safeguard measures with regard to third countries for a period not exceeding six months if such measures are strictly necessary.

TITeL V
AREA OF FREEDOM, SECURITY AND JUSTICE

CHAPTER 4
JUDICIAL COOPERATION IN CRIMINAL MATTERS

Article 83
1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

TITeL VIII
ECONOMIC AND MONETARY POLICY

Article 119
1. For the purposes set out in Article 3 of the Treaty on European Union, the activities of the Member States and the Union shall include, as provided in the Treaties, the adoption of an economic policy which is based on the close coordination of Member States’ economic policies, on the internal market and on the definition of common objectives, and conducted in accordance with the principle of an open market economy with free competition.

2. Concurrently with the foregoing, and as provided in the Treaties and in accordance with the procedures set out therein, these activities shall include a single currency, the euro, and the definition and conduct of a single monetary policy and exchange-rate policy the primary objective of both of which shall be to maintain price stability and, without prejudice to this objective, to support the general economic policies in the Union, in accordance with the principle of an open market economy with free competition.

3. These activities of the Member States and the Union shall entail compliance with the following guiding principles: stable prices, sound public finances and monetary conditions and a sustainable balance of payments.

CHAPeR 2
MONETARY POLICY

Article 127
1. The primary objective of the European System of Central Banks (hereinafter referred to as ‘the ESCB’) shall be to maintain price stability. Without prejudice to the objective of price stability, the ESCB shall support the general economic policies in the Union with a view to contributing to the achievement of the objectives of the Union as laid down in Article 3 of the Treaty on European Union. The ESCB shall act in accordance with the principle of an open market economy with free competition, favouring an efficient allocation of resources, and in compliance with the principles set out in Article 119.

2. The basic tasks to be carried out through the ESCB shall be:

— to define and implement the monetary policy of the Union,
— to conduct foreign-exchange operations consistent with the provisions of Article 219,
— to hold and manage the official foreign reserves of the Member States,
— to promote the smooth operation of payment systems.

3. The third indent of paragraph 2 shall be without prejudice to the holding and management by the governments of Member States of foreign-exchange working balances.

4. The European Central Bank shall be consulted:

— on any proposed Union act in its fields of competence,
— by national authorities regarding any draft legislative provision in its fields of competence, but within the limits and under the conditions set out by the Council in accordance with the procedure laid down in Article 129(4).

The European Central Bank may submit opinions to the appropriate Union institutions, bodies, offices or agencies or to national authorities on matters in its fields of competence.

5. The ESCB shall contribute to the smooth conduct of policies pursued by the competent authorities relating to the prudential supervision of credit institutions and the stability of the financial system.

6. The Council, acting by means of regulations in accordance with a special legislative procedure, may unanimously, and after consulting the European Parliament and the European Central Bank, confer specific tasks upon the European Central Bank concerning policies relating to the prudential supervision of credit institutions and other financial institutions with the exception of insurance undertakings.

Article 128
1. The European Central Bank shall have the exclusive right to authorise the issue of 360 banknotes within the Union. The European Central Bank and the national central banks may issue such notes. The banknotes issued by the European Central Bank and the national central banks shall be the only such notes to have the status of legal tender within the Union.

2. Member States may issue euro coins subject to approval by the European Central Bank of the volume of the issue. The Council, on a proposal from the Commission and after consulting the European Parliament and the European Central Bank, may adopt measures to harmonise the denominations and technical specifications of all coins intended for circulation to the extent necessary to permit their smooth circulation within the Union.

Article 129
1. The ESCB shall be governed by the decision-making bodies of the European Central Bank which shall be the Governing Council and the Executive Board.

2. The Statute of the European System of Central Banks and of the European Central Bank (hereinafter referred to as ‘the Statute of the ESCB and of the ECB’) is laid down in a Protocol annexed to the Treaties.

3. Articles 5, 8, 12, 17, 18, 19.1, 20, 23, 24, 26, 32.2, 33.1, 32.4, 32.6, 33.1(a) and 36 of the Statute of the ESCB and of the ECB may be amended by the European Parliament and the Council, acting in accordance with the ordinary legislative procedure. They shall act either on a recommendation from the European Central Bank and after consulting the Commission or on a proposal from the Commission and after consulting the European Central Bank.

4. The Council, on a proposal from the Commission and after consulting the European Parliament and the European Central Bank or on a recommendation from the European Central Bank and after consulting the European Parliament and the Commission, shall adopt the provisions referred to in Articles 4, 5, 19.2, 20, 28.1, 29.2, 30.4 and 34.3 of the Statute of the ESCB and of the ECB.

Article 130
When exercising the powers and carrying out the tasks and duties conferred upon them by the Treaties and the Statute of the ESCB and of the ECB, neither the European Central Bank, nor a national central bank, nor any member of their decision-making bodies shall seek or take instructions from Union institutions, bodies, offices or agencies, from any government of a Member State or from any other body. The Union institutions, bodies, offices or agencies and the governments of the Member States undertake to respect this principle and not to seek to influence the members of the decision-making bodies of the European Central Bank or of the national central banks in the performance of their tasks.

Article 131
Each Member State shall ensure that its national legislation including the statutes of its national central bank is compatible with the Treaties and the Statute of the ESCB and of the ECB.

Article 132
1. In order to carry out the tasks entrusted to the ESCB, the European Central Bank shall, in accordance with the provisions of the Treaties and under the conditions laid down in the Statute of the ESCB and of the ECB:

   — make regulations to the extent necessary to implement the tasks defined in Article 3.1, first indent, Articles 19.1, 22 and 25.2 of the Statute of the ESCB and of the ECB in cases which shall be laid down in the acts of the Council referred to in Article 129(4),

   — take decisions necessary for carrying out the tasks entrusted to the ESCB under the Treaties and the Statute of the ESCB and of the ECB,

   — make recommendations and deliver opinions.

2. The European Central Bank may decide to publish its decisions, recommendations and opinions.

3. Within the limits and under the conditions adopted by the Council under the procedure laid down in Article 129(4), the European Central Bank shall be entitled to impose fines or periodic penalty payments on undertakings for failure to comply with obligations under its regulations and decisions.

Article 133
Without prejudice to the powers of the European Central Bank, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the measures necessary for the use of the euro as the single currency. Such measures shall be adopted after consultation of the European Central Bank.

—

CHAPTER 4
PROVISIONS SPECIFIC TO MEMBER STATES WHOSE CURRENCY IS THE EURO

Article 136
1. In order to ensure the proper functioning of economic and monetary union, and in accordance with the relevant provisions of the Treaties, the Council shall, in accordance with the relevant procedure from among those referred to in Articles 121 and 126, with the exception of the procedure set out in Article 126(14), adopt measures specific to those Member States whose currency is the euro:

   (a) to strengthen the coordination and surveillance of their budgetary discipline;

   (b) to set out economic policy guidelines for them, while ensuring that they are compatible with those adopted for the whole of the Union and are kept under surveillance.

2. For those measures set out in paragraph 1, only members of the Council representing Member States whose currency is the euro shall take part in the vote.

A qualified majority of the said members shall be defined in accordance with Article 238(3)(a).

—

Article 138
1. In order to secure the euro's place in the international monetary system, the Council, on a proposal from the Commission, shall adopt a decision establishing common positions on matters of particular interest for economic and monetary union within the competent international financial institutions and conferences. The Council shall act after consulting the European Central Bank.

2. The Council, on a proposal from the Commission, may adopt appropriate measures to ensure unified representation within
the international financial institutions and conferences. The Council shall act after consulting the European Central Bank.

3. For the measures referred to in paragraphs 1 and 2, only members of the Council representing Member States whose currency is the euro shall take part in the vote.

A qualified majority of the said members shall be defined in accordance with Article 238(3)(a).

CHAPTER 5
TRANSITIONAL PROVISIONS

Article 139
1. Member States in respect of which the Council has not decided that they fulfil the necessary conditions for the adoption of the euro shall hereinafter be referred to as ‘Member States with a derogation’.

2. The following provisions of the Treaties shall not apply to Member States with a derogation:
   (a) adoption of the parts of the broad economic policy guidelines which concern the euro area generally (Article 121(2));
   (b) coercive means of remedying excessive deficits (Article 126(9) and (11));
   (c) the objectives and tasks of the ESCB (Article 127(1) to (3) and (5));
   (d) issue of the euro (Article 128);
   (e) acts of the European Central Bank (Article 132);
   (f) monetary agreements and other measures relating to exchange-rate policy (Article 219);
   (g) appointment of members of the Executive Board of the European Central Bank (Article 283(2));
   (i) decisions establishing common positions on issues of particular relevance for economic and monetary union within the competent international financial institutions and conferences (Article 138(1));
   (j) measures to ensure unified representation within the international financial institutions and conferences (Article 138(2)).

In the Articles referred to in points (a) to (j), ‘Member States’ shall therefore mean Member States whose currency is the euro.

3. Under Chapter IX of the Statute of the ESCB and of the ECB, Member States with a derogation and their national central banks are excluded from rights and obligations within the ESCB.

4. The voting rights of members of the Council representing Member States with a derogation shall be suspended for the adoption by the Council of the measures referred to in the Articles listed in paragraph 2, and in the following instances:
   (a) recommendations made to those Member States whose currency is the euro in the framework of multilateral surveillance, including on stability programmes and warnings (Article 121(4));
   (b) measures relating to excessive deficits concerning those Member States whose currency is the euro (Article 126(6), (7), (8), (12) and (13)).

A qualified majority of the other members of the Council shall be defined in accordance with Article 238(3)(a).

Article 140
1. At least once every two years, or at the request of a Member State with a derogation, the Commission and the European Central Bank shall report to the Council on the progress made by the Member States with a derogation in fulfilling their obligations regarding the achievement of economic and monetary union. These reports shall include an examination of the compatibility between the national legislation of each of these Member States, including the statutes of its national central bank, and Articles 130 and 131 and the Statute of the ESCB and of the ECB. The reports shall also examine the achievement of a high degree of sustainable convergence by reference to the fulfilment by each Member State of the following criteria:

   — the achievement of a high degree of price stability; this will be apparent from a rate of inflation which is close to that of, at most, the three best performing Member States in terms of price stability,
   — the sustainability of the government financial position; this will be apparent from having achieved a government budgetary position without a deficit that is excessive as determined in accordance with Article 126(6),
   — the observance of the normal fluctuation margins provided for by the exchange-rate mechanism of the European Monetary System, for at least two years, without deviating against the euro,
   — the durability of convergence achieved by the Member State with a derogation and of its participation in the exchange-rate mechanism being reflected in the long-term interest-rate levels.

The four criteria mentioned in this paragraph and the relevant periods over which they are to be respected are developed further in a Protocol annexed to the Treaties. The reports of the Commission and the European Central Bank shall also take account of the results of the integration of markets, the situation and development of the balances of payments on current account and an examination of the development of unit labour costs and other price indices.

2. After consulting the European Parliament and after discussion in the European Council, the Council shall, on a proposal from the Commission, decide which Member States with a derogation fulfil the necessary conditions on the basis of the criteria set out in paragraph 1, and abrogate the derogations of the Member States concerned.

The Council shall act having received a recommendation of a qualified majority of those among its members representing Member States whose currency is the euro. These members shall act within six months of the Council receiving the Commission’s proposal.

The qualified majority of the said members, as referred to in the second subparagraph, shall be defined in accordance with Article 238(3)(a).

3. If it is decided, in accordance with the procedure set out in paragraph 2, to abrogate a derogation, the Council shall, acting with the unanimity of the Member States whose currency is the euro and the Member State concerned, on a proposal from the Commission and after consulting the European Central Bank, irrevocably fix the rate at which the euro shall be substituted for the currency of the Member State concerned, and take the other measures necessary for the introduction of the euro as the single currency in the Member State concerned.

Article 141
1. If and as long as there are Member States with a derogation, and without prejudice to Article 129(1), the General Council of the European Central Bank referred to in Article 44 of the Statute of the ESCB and of the ECB shall be constituted as a third decision-making body of the European Central Bank.

2. If and as long as there are Member States with a derogation, the European Central Bank shall, as regards those Member States:

   — strengthen cooperation between the national central banks,
   — strengthen the coordination of the monetary policies of the Member States, with the aim of ensuring price stability,
   — monitor the functioning of the exchange-rate mechanism,
   — hold consultations concerning issues falling within the competence of the national central banks and affecting the stability of financial institutions and markets,
   — carry out the former tasks of the European Monetary Cooperation Fund which had subsequently been taken over by the European Monetary Institute.

Article 142
Each Member State with a derogation shall treat its exchange-rate policy as a matter of common interest. In so doing, Member States shall take account of the experience acquired
in cooperation within the framework of the exchange-rate mechanism.

Article 143
1. Where a Member State with a derogation is in difficulties or is seriously threatened with difficulties as regards its balance of payments either as a result of an overall disequilibrium in its balance of payments, or as a result of the type of currency at its disposal, and where such difficulties are liable in particular to jeopardise the functioning of the internal market or the implementation of the common commercial policy, the Commission shall immediately investigate the position of the State in question and the action which, making use of all the means at its disposal, that State has taken or may take in accordance with the provisions of the Treaties. The Commission shall state what measures it recommends the State concerned to take.

If the action taken by a Member State with a derogation and the measures suggested by the Commission do not prove sufficient to overcome the difficulties which have arisen or which threaten, the Commission shall, after consulting the Economic and Financial Committee, recommend to the Council the granting of mutual assistance and appropriate methods therefor.

The Commission shall keep the Council regularly informed of the situation and of how it is developing.

[...]

Article 144
1. Where a sudden crisis in the balance of payments occurs and a decision within the meaning of Article 143(2) is not immediately taken, a Member State with a derogation may, as a precaution, take the necessary protective measures. Such measures must cause the least possible disturbance in the functioning of the internal market and must not be wider in scope than is strictly necessary to remedy the sudden difficulties which have arisen.

2. The Commission and the other Member States shall be informed of such protective measures not later than when they enter into force. The Commission may recommend to the Council the granting of mutual assistance under Article 143.

3. After the Commission has delivered a recommendation and the Economic and Financial Committee has been consulted, the Council may decide that the Member State concerned shall amend, suspend or abolish the protective measures referred to above.

PART SIX
INSTITUTIONAL AND FINANCIAL PROVISIONS

TITLE I
INSTITUTIONAL PROVISIONS

CHAPTER 1
THE INSTITUTIONS

SECTION 6
THE EUROPEAN CENTRAL BANK

Article 282
1. The European Central Bank, together with the national central banks, shall constitute the European System of Central Banks (ESCB). The European Central Bank, together with the national central banks of the Member States whose currency is the euro, which constitute the Eurosystem, shall conduct the monetary policy of the Union.

2. The ESCB shall be governed by the decision-making bodies of the European Central Bank. The primary objective of the ESCB shall be to maintain price stability. Without prejudice to that objective, it shall support the general economic policies in the Union in order to contribute to the achievement of the latter’s objectives.

3. The European Central Bank shall have legal personality. It alone may authorise the issue of the euro. It shall be independent in the exercise of its powers and in the management of its finances. Union institutions, bodies, offices and agencies and the governments of the Member States shall respect that independence.

4. The European Central Bank shall adopt such measures as are necessary to carry out its tasks in accordance with Articles 127 to 133, with Article 138, and with the conditions laid down in the Statute of the ESCB and of the ECB. In accordance with these same Articles, those Member States whose currency is not the euro, and their central banks, shall retain their powers in monetary matters.

5. Within the areas falling within its responsibilities, the European Central Bank shall be consulted on all proposed Union acts, and all proposals for regulation at national level, and may give an opinion.

Article 283
1. The Governing Council of the European Central Bank shall comprise the members of the Executive Board of the European Central Bank and the Governors of the national central banks of the Member States whose currency is the euro.

2. The Executive Board shall comprise the President, the Vice-President and four other members.

The President, the Vice-President and the other members of the Executive Board shall be appointed by the European Council, acting by a qualified majority, from among persons of recognised standing and professional experience in monetary or banking matters, on a recommendation from the Council, after it has consulted the European Parliament and the Governing Council of the European Central Bank.

Their term of office shall be eight years and shall not be renewable.

Only nationals of Member States may be members of the Executive Board.

Article 284
1. The President of the Council and a Member of the Commission may participate, without having the right to vote, in meetings of the Governing Council of the European Central Bank.

The President of the Council may submit a motion for deliberation to the Governing Council of the European Central Bank.

2. The President of the European Central Bank shall be invited to participate in Council meetings when the Council is discussing matters relating to the objectives and tasks of the ESCB.

3. The European Central Bank shall address an annual report on the activities of the ESCB and on the monetary policy of both the previous and current year to the European Parliament, the Council and the Commission, and also to the European Council. The President of the European Central Bank shall present this report to the Council and to the European Parliament, which may hold a general debate on that basis.

The President of the European Central Bank and the other members of the Executive Board may, at the request of the European Parliament or on their own initiative, be heard by the competent committees of the European Parliament.

(Editorial note: More articles of this treaty may be found in the part I E-Commerce.)
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47(2), Article 55 and Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) It is important, in the context of achieving the aims of the single market, to adopt measures designed to consolidate progressively this market and those measures must contribute to attaining a high level of consumer protection, in accordance with Articles 95 and 153 of the Treaty.

(2) Both for consumers and suppliers of financial services, the distance marketing of financial services will constitute one of the main tangible results of the completion of the internal market.

(3) Within the framework of the internal market, it is in the interest of consumers to have access without discrimination to the widest possible range of financial services available in the Community so that they can choose those that are best suited to their needs. In order to safeguard freedom of choice, which is an essential consumer right, a high degree of consumer protection is required in order to enhance consumer confidence in distance selling.

(4) It is essential to the smooth operation of the internal market for consumers to be able to negotiate and conclude contracts with a supplier established in other Member States, regardless of whether the supplier is also established in the Member State in which the consumer resides.

(5) Because of their intangible nature, financial services are particularly suited to distance selling and the establishment of a legal framework governing the distance marketing of financial services should increase consumer confidence in the use of new techniques for the distance marketing of financial services, such as electronic commerce.

(6) This Directive should be applied in conformity with the Treaty and with secondary law, including Directive 2000/31/EC (4) on electronic commerce, the latter being applicable solely to the transactions which it covers.

(7) This Directive aims to achieve the objectives set forth above without prejudice to Community or national law governing freedom to provide services or, where applicable, host Member State control and/or authorisation or supervision systems in the Member States where this is compatible with Community legislation.

(8) Moreover, this Directive, and in particular its provisions relating to information about any contractual clause on law applicable to the contract and/or on the competent court does not affect the applicability to the distance marketing of consumer financial services of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (5) or of the 1980 Rome Convention on the law applicable to contractual obligations.

(9) The achievement of the objectives of the Financial Services Action Plan requires a higher level of consumer protection in certain areas. This implies a greater convergence, in particular, in non harmonised collective investment funds, rules of conduct applicable to investment services and consumer credits. Pending the achievement of the above convergence, a high level of consumer protection should be maintained.

(10) Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (6) lays down the main rules applicable to distance contracts for goods or services concluded between a supplier and a consumer. However, that Directive does not cover financial services.

(11) In the context of the analysis conducted by the Commission with a view to ascertaining the need for specific measures in the field of financial services, the Commission invited all the interested parties to transmit their comments, notably in connection with the preparation of its Green Paper entitled 'Financial Services — Meeting Consumers' Expectations'. The consultations in this context showed that there is a need to strengthen consumer protection in this area. The Commission therefore decided to present a specific proposal concerning the distance marketing of financial services.

(12) The adoption by the Member States of conflicting or different consumer protection rules governing the distance marketing of consumer financial services could impede the functioning of the internal market and competition between firms in the market. It is therefore necessary to enact common rules at Community level in this area, consistent with no reduction in overall consumer protection in the Member States.

(13) A high level of consumer protection should be guaranteed by this Directive, with a view to ensuring the free movement of financial services. Member States should not be able to adopt provisions other than those laid down in this Directive in the fields it harmonises, unless otherwise specifically indicated in it.

(14) This Directive covers all financial services liable to be provided at a distance. However, certain financial services are governed by specific provisions of Community legislation which continue to apply to those financial services. However, principles governing the distance marketing of such services should be laid down.

(15) Contracts negotiated at a distance involve the use of means of distance communication which are used as part of a distance sales or service-provision scheme not involving the simultaneous presence of the supplier and the consumer. The constant development of those means of communication requires principles to be defined that are valid even for those means which are not yet in widespread use. Therefore, distance contracts are those the offer, negotiation and conclusion of which are carried out at a distance.

(16) A single contract involving successive operations or separate operations of the same nature performed over time may be subject to different legal treatment in the different Member States, but it is important that this Directive be applied in the same way in all the Member States. To that end, it is appropriate that this Directive should be considered to apply to the first of a series of successive operations or separate operations of the same nature performed over time which may be considered as forming a whole, irrespective of whether that operation or series of operations is the subject of a single contract or several successive contracts.

(17) An 'initial service agreement' may be considered to be for example the deposit or withdrawal of funds to or from the bank account, payment by credit card, transactions made within the framework of a
portfolios management contract. Adding new elements to an initial service agreement, such as a possibility to use an electronic payment instrument together with one’s existing bank account, does not constitute an ‘operation’ but an additional contract to which this Directive applies. The subscription to new units of the same collective investment fund is considered to be one of ‘successive operations of the same nature’.

(19) By covering a service-provision scheme organised by the financial services provider, this Directive aims to exclude from its scope services provided on a strictly occasional basis and outside a commercial structure dedicated to the conclusion of distance contracts.

(19)The supplier is the person providing services at a distance. This Directive should however also apply when one of the marketing stages involves an intermediary. Having regard to the nature and degree of that involvement, the pertinent provisions of this Directive should apply to such an intermediary, irrespective of his or her legal status.

(20) Durable media include in particular floppy discs, CD-ROMs, DVDs and the hard drive of the consumer’s computer on which the electronic mail is stored, but they do not include Internet websites unless they fulfil the criteria contained in the definition of a durable medium.

(21) The use of means of distance communications should not lead to an unwarranted restriction on the information provided to the client. In the interests of transparency this Directive lays down the requirements needed to ensure that an appropriate level of information is provided to the consumer both before and after conclusion of the contract. The consumer should receive, before conclusion of the contract, the prior information needed so as to properly appraise the financial service offered to him and hence make a well-informed choice. The supplier should specify how long his offer applies as it stands.

(22) Information items listed in this Directive cover information of a general nature applicable to all kinds of financial services. Other information requirements concerning a given financial service, such as the coverage of an insurance policy, are not solely specified in this Directive. This kind of information should be provided in accordance, where applicable, with relevant Community legislation or national legislation in conformity with Community law.

(23) With a view to optimum protection of the consumer, it is important that the consumer is adequately informed of the provisions of this Directive and of any codes of conduct existing in this area and that he has a right of withdrawal.

(24) When the right of withdrawal does not apply because the consumer has expressly requested the performance of a contract, the supplier should inform the consumer of this fact.

(25) Consumers should be protected against unsolicited services. Consumers should be exempt from any obligation in the case of unsolicited services, the absence of a reply not being construed as signifying consent on their part. However, this rule should be without prejudice to the tacit renewal of contracts validly concluded between the parties whenever the law of the Member States permits such tacit renewal.

(26) Member States should take appropriate measures to protect effectively consumers who do not wish to be contacted through certain means of communication or at certain times. This Directive should be without prejudice to the particular safeguards available to consumers under Community legislation concerning the protection of personal data and privacy.

(27) With a view to protecting consumers, there is a need for suitable and effective complaint and redress procedures in the Member States with a view to settling potential disputes between suppliers and consumers, by using, where appropriate, existing procedures.

(28) Member States should encourage public or private bodies established with a view to settling disputes out of court to cooperate in resolving cross-border disputes. Such cooperation could in particular entail allowing consumers to submit to extra-judicial bodies in the Member State of their residence complaints concerning suppliers established in other Member States. The establishment of FIN-NET offers increased assistance to consumers when using cross-border services.

(29) This Directive is without prejudice to extension by Member States, in accordance with Community law, of the protection provided by this Directive to non-profit organisations and persons making use of financial services in order to become entrepreneurs.

(30) This Directive should also cover cases where the national legislation includes the concept of a consumer making a binding contractual statement.

(31) The provisions in this Directive on the supplier’s choice of language should be without prejudice to provisions of national legislation, adopted in conformity with Community law governing the choice of language.

(32) The Community and the Member States have entered into commitments in the context of the General Agreement on Trade in Services (GATS) concerning the possibility for consumers to purchase banking and investment services abroad. The GATS entitles Member States to adopt measures for prudential reasons, including measures to protect investors, depositors, policy-holders and persons to whom a financial service is owed by the supplier of the financial service. Such measures should not impose restrictions going beyond what is required to ensure the protection of consumers.

(33) In view of the adoption of this Directive, the scope of Directive 97/7/EC and Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers’ interests (7) and the scope of the cancellation period in Council Directive 90/619/EEC of 8 November 1990 on the coordination of laws, regulations and administrative provisions relating to direct life assurance, laying down provisions to facilitate the effective exercise of freedom to provide services (8) should be adapted.

(34) Since the objectives of this Directive, namely the establishment of common rules on the distance marketing of consumer financial services cannot be sufficiently achieved by the Member States and can therefore be better achieved at Community level, the Community may adopt measures, in accordance with the principles of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary to achieve that objective.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Object and scope

1. The object of this Directive is to approximate the laws, regulations and administrative provisions of the Member States concerning the distance marketing of consumer financial services.

2. In the case of contracts for financial services comprising an initial service agreement followed by successive operations or a series of separate operations of the same nature performed over time, the provisions of this Directive shall apply only to the initial agreement.

In this case there is no initial service agreement but the successive operations or the separate operations of the same nature performed over time are performed between the same contractual parties, Articles 3 and 4 apply only when the first operation is performed. Where, however, no operation of the same nature is performed for more than one year, the next operation will be deemed to be the first in a new series of operations and, accordingly, Articles 3 and 4 shall apply.

Article 2

Definitions

For the purposes of this Directive:
(a) ‘distance contract’ means any contract concerning financial services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who, for the purpose of that contract, makes exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;

(b) ‘financial service’ means any service of a banking, credit, insurance, personal pension, investment or payment nature;

(c) ‘supplier’ means any natural or legal person, public or private, who, acting in his commercial or professional capacity, is the contractual provider of services subject to distance contracts;

(d) ‘consumer’ means any natural person who, in distance contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession;

(e) ‘means of distance communication’ refers to any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the distance marketing of a service between those parties;

(f) ‘durable medium’ means any instrument which enables the consumer to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(g) ‘operator or supplier of a means of distance communication’ means any public or private, natural or legal person whose trade, business or profession involves making one or more means of distance communication available to suppliers.

Article 3

Information to the consumer prior to the conclusion of the distance contract

1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

(a) the identity and the main business of the supplier, the geographical address at which the supplier is established and any other geographical address relevant for the customer’s relations with the supplier;

(b) the identity of the representative of the supplier established in the consumer’s Member State of residence and the geographical address relevant for the customer’s relations with the representative, if such a representative exists;

(c) when the consumer’s dealings are with any professional other than the supplier, the identity of this professional, the capacity in which he is acting vis-à-vis the consumer, and the geographical address relevant for the customer’s relations with this professional;

(d) where the supplier is registered in a trade or similar public register, the trade register in which the supplier is entered and his registration number or an equivalent means of identification in that register;

(e) where the supplier’s activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(2) the financial service

(a) a description of the main characteristics of the financial service;

(b) the total price to be paid by the consumer to the supplier for the financial service, including all related fees, charges and expenses, and all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it;

(c) where relevant notice indicating that the financial service is related to instruments involving special risks related to their specific features or the operations to be executed or whose price depends on fluctuations in the financial markets outside the supplier’s control and that historical performances are no indicators for future performances;

(d) notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him;

(e) any limitations of the period for which the information provided is valid;

(f) the arrangements for payment and for performance;

(g) any specific additional cost for the consumer of using the means of distance communication, if such additional cost is charged;

(3) the distance contract

(a) the existence or absence of a right of withdrawal in accordance with Article 6 and, where the right of withdrawal exists, its duration and the conditions for exercising it, including information on the amount which the consumer may be required to pay on the basis of Article 7(1), as well as the consequences of non-exercise of that right;

(b) the minimum duration of the distance contract in the case of financial services to be performed permanently or recurrently;

(c) information on any rights the parties may have to terminate the contract early or unilaterally by virtue of the terms of the distance contract, including any penalties imposed by the contract in such cases;

(d) practical instructions for exercising the right of withdrawal indicating, inter alia, the address to which the notification of a withdrawal should be sent;

(e) the Member State or States whose laws are taken by the supplier as a basis for the establishment of relations with the consumer prior to the conclusion of the distance contract;

(f) any contractual clause on law applicable to the distance contract and/or on competent court;

(g) in which language, or languages, the contractual terms and conditions, and the prior information referred to in this Article are supplied, and furthermore in which language, or languages, the supplier, with the agreement of the consumer, undertakes to communicate during the duration of this distance contract;

(4) redress

(a) whether or not there is an out-of-court complaint and redress mechanism for the consumer that is party to the distance contract and, if so, the methods for having access to it;

(b) the existence of guarantee funds or other compensation arrangements, not covered by Directive 94/19/EC of the European Parliament and of the Council of 30 May 1994 on deposit guarantee schemes ( 9 ) and Directive 97/9/EC of the European Parliament and of the Council of 3 March 1997 on investor compensation schemes ( 10 );

2. The information referred to in paragraph 1, the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions, and the principles governing the protection of those who are unable, pursuant to the legislation of the Member States, to give their consent, such as minors.

3. In the case of voice telephony communications

(a) the identity of the supplier and the commercial purpose of the call initiated by the supplier shall be made explicitly clear at the beginning of any conversation with the consumer;

(b) subject to the explicit consent of the consumer only the following information needs to be given:

— the identity of the person in contact with the consumer and his link with the supplier,

— a description of the main characteristics of the financial service,

— the total price to be paid by the consumer to the supplier for the financial service including all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it,

— notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him,
the existence or absence of a right of withdrawal in accordance with Article 6 and, where the right of withdrawal exists, its duration and the conditions for exercising it, including information on the amount which the consumer may be required to pay on the basis of Article 7(1).

The supplier shall inform the consumer that other information is available on request and of what nature this information is. In any case the supplier shall provide the full information when he fulfils his obligations under Article 5.

4. Information on contractual obligations, to be communicated to the consumer during the pre-contractual phase, shall be in conformity with the contractual obligations which would result from the law presumed to be applicable to the distance contract if the latter were concluded.

Article 4
Additional information requirements
1. Where there are provisions in the Community legislation governing financial services which contain prior information requirements additional to those listed in Article 3(1), these requirements shall continue to apply.
2. Pending further harmonisation, Member States may maintain or introduce more stringent provisions on prior information requirements when the provisions are in conformity with Community law.
3. Member States shall communicate to the Commission national provisions on prior information requirements under paragraphs 1 and 2 of this Article when these requirements are additional to those listed in Article 3(1). The Commission shall take account of the communicated national provisions when drawing up the report referred to in Article 20(2).
4. The Commission shall, with a view to creating a high level of transparency by all appropriate means, ensure that information, on the national provisions communicated to it, is made available to consumers and suppliers.

Article 5
Communication of the contractual terms and conditions and of the prior information
1. The supplier shall communicate to the consumer all the contractual terms and conditions and the information referred to in Article 3(1) and Article 4 on paper or on another durable medium available and accessible to the consumer in good time before the consumer is bound by any distance contract or offer.
2. The supplier shall fulfils his obligation under paragraph 1 immediately after the conclusion of the contract, if the contract has been concluded at the consumer’s request using a means of distance communication which does not enable providing the contractual terms and conditions and the information in conformity with paragraph 1.
3. At any time during the contractual relationship the consumer is entitled, at his request, to receive the contractual terms and conditions on paper. In addition, the consumer is entitled to change the means of distance communication used, unless this is incompatible with the contract concluded or the nature of the financial service provided.

Article 6
Right of withdrawal
1. The Member States shall ensure that the consumer shall have a period of 14 calendar days to withdraw from the contract without penalty and without giving any reason. However, this period shall be extended to 30 calendar days in distance contracts relating to life insurance covered by Directive 90/6/EC and personal pension operations.

The period for withdrawal shall begin:

— either from the day of the conclusion of the distance contract, except in respect of the said life assurance, where the time limit will begin from the time when the consumer is informed that the distance contract has been concluded, or
— from the day on which the consumer receives the contractual terms and conditions and the information in accordance with Article 5(1) or (2), if that is later than the date referred to in the first indent.

Member States, in addition to the right of withdrawal, may provide that the enforceability of contracts relating to investment services is suspended for the same period provided for in this paragraph.

2. The right of withdrawal shall not apply to:

(a) financial services whose price depends on fluctuations in the financial market outside the suppliers control, which may occur during the withdrawal period, such as services related to:
— foreign exchange,
— money market instruments,
— transferable securities,
— units in collective investment undertakings,
— financial-futures contracts, including equivalent cash-settled instruments,
— forward interest-rate agreements (FRAs),
— interest-rate, currency and equity swaps,
— options to acquire or dispose of any instruments referred to in this point including equivalent cash-settled instruments. This category includes in particular options on currency and on interest rates;
(b) travel and baggage insurance policies or similar short-term insurance policies of less than one month’s duration;
(c) contracts whose performance has been fully completed by both parties at the consumer’s express request before the consumer exercises his right of withdrawal.

3. Member States may provide that the right of withdrawal shall not apply to:

(a) any credit intended primarily for the purpose of acquiring or retaining property rights in land or in an existing or projected building, or for the purpose of renovating or improving a building, or
(b) any credit secured either by mortgage on immovable property or by a right related to immovable property, or
(c) declarations by consumers using the services of an official, provided that the official confirms that the consumer is guaranteed the rights under Article 5(1).

This paragraph shall be without prejudice to the right to a reflection time to the benefit of the consumers that are resident in those Member States where it exists, at the time of the adoption of this Directive.

4. Member States making use of the possibility set out in paragraph 3 shall communicate it to the Commission.

5. The Commission shall make available the information communicated by Member States to the European Parliament and the Council and shall ensure that it is also available to consumers and suppliers who request it.

6. If the consumer exercises his right of withdrawal he shall, before the expiry of the relevant deadline, notify this following the practical instructions given to him in accordance with Article 3(1)(3)(d) by means which can be proved in accordance with national law. The deadline shall be deemed to have been observed if the notification, if it is on paper or on another durable medium available and accessible to the recipient, is dispatched before the deadline expires.

7. This Article does not apply to credit agreements cancelled under the conditions of Article 6(4) of Directive 97/7/EC or Article 7 of Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of the right to use immovable properties on a timeshare basis (12).

If to a distance contract of a given financial service another distance contract has been attached concerning services provided by the supplier or by a third party on the basis of
an agreement between the third party and the supplier, this additional distance contract shall be cancelled, without any penalty, if the consumer exercises his right of withdrawal as provided for in Article 6(1).

8. The provisions of this Article are without prejudice to the Member States’ laws and regulations governing the cancellation or termination or non-enforceability of a distance contract or the right of a consumer to fulfil his contractual obligations before the time fixed in the distance contract. This applies irrespective of the conditions for and the legal effects of the winding-up of the contract.

Article 7
Payment of the service provided before withdrawal
1. When the consumer exercises his right of withdrawal under Article 6(1) he may only be required to pay, without any undue delay, for the service actually provided by the supplier in accordance with the contract. The performance of the contract may only begin after the consumer has given his approval. The amount payable shall not:
   — exceed an amount which is in proportion to the extent of the service already provided in comparison with the full coverage of the contract,
   — in any case be such that it could be construed as a penalty.
2. Member States may provide that the consumer cannot be required to pay any amount when withdrawing from an insurance contract.
3. The supplier may not require the consumer to pay any amount on the basis of paragraph 1 unless he can prove that the consumer was duly informed about the amount payable, in conformity with Article 3(1)(3)(a). However, in no case may he require such payment if he has commenced the performance of the contract before the expiry of the withdrawal period provided for in Article 6(1) without the consumer’s prior request.
4. The supplier shall, without any undue delay and no later than within 30 calendar days, return to the consumer any sums he has received from him in accordance with the distance contract, except for the amount referred to in paragraph 1. This period shall begin from the day on which the supplier receives notice of withdrawal.
5. The consumer shall return to the supplier any sums and/or property he has received from the supplier without any undue delay and no later than within 30 calendar days. This period shall begin from the day on which the consumer dispatches the notification of withdrawal.

Article 9

Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (13) and without prejudice to the provisions of Member States’ legislation on the tacit renewal of distance contracts, when such rules permit tacit renewal, Member States shall take measures to exempt the consumer from any obligation in the event of unsolicited supplies, the absence of a reply not constituting consent.

Article 10
Unsolicited communications
1. The use by a supplier of the following distance communication techniques shall require the consumer’s prior consent:
   (a) automated calling systems without human intervention (automatic calling machines);
   (b) fax machines.
2. Member States shall ensure that means of distance communication other than those referred to in paragraph 1, when they allow individual communications:
   (a) shall not be authorised unless the consent of the consumers concerned has been obtained, or
   (b) may only be used if the consumer has not expressed his manifest objection.
3. The measures referred to in paragraphs 1 and 2 shall not entail costs for consumers.

Article 11
Sanctions
Member States shall provide for appropriate sanctions in the event of the supplier’s failure to comply with national provisions adopted pursuant to this Directive. They may provide for this purpose in particular that the consumer may cancel the contract at any time, free of charge and without penalty.

These sanctions must be effective, proportional and dissuasive.

Article 12
Impressive nature of the Directive’s provisions
1. Consumers may not waive the rights conferred upon them by this Directive.
2. Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-member country as the law applicable to the contract, if this contract has a close link with the territory of one or more Member States.

Article 13
Judicial and administrative redress
1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive in the interests of consumers.
2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action in accordance with national law before the courts or competent administrative bodies to ensure that the national provisions for the implementation of this Directive are applied:
   (a) public bodies or their representatives;
   (b) consumer organisations having a legitimate interest in protecting consumers;
   (c) professional organisations having a legitimate interest in acting.
3. Member States shall take the measures necessary to ensure that operators and suppliers of means of distance communication put an end to practices that have been declared to be contrary to this Directive, on the basis of a judicial decision, an administrative decision or a decision issued by a supervisory authority notified to them, where those operators or suppliers are in a position to do so.

Article 14
Out-of-court redress
1. Member States shall promote the setting up or development of adequate and effective out-of-court complaints and redress procedures for the settlement of consumer disputes concerning financial services provided at distance.
2. Member States shall, in particular, encourage the bodies responsible for out-of-court settlement of disputes to cooperate in the resolution of cross-border disputes concerning financial services provided at distance.

Article 15
Burden of proof
Without prejudice to Article 7(3), Member States may stipulate that the burden of proof in respect of the supplier’s obligations to inform the consumer and the consumer’s consent to conclusion of the contract and, where appropriate, its performance, can be placed on the supplier. Any contractual term or condition providing that the burden of proof of the respect by the supplier of all or part of the obligations incumbent on him pursuant to this Directive should lie with the consumer shall be an unfair term within the meaning of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (14).

Article 16
Transitional measures
... (edited) ...
Entry into force
This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 23
Addressees
This Directive is addressed to the Member States.


Amended by:

  - OJ L 149, 22.05.2005
  - OJ L 319, 13.11.2007


THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European CoTHE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47(2) thereof,

Having regard to the proposal from the Commission (1),

Having regard to the Opinion of the European Economic and Social Committee (2),

Having regard to the opinion of the European Central Bank (3),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (4),

Whereas:

(2) In recent years more investors have become active in the financial markets and are offered an even more complex wide-ranging set of services and instruments. In view of these developments the legal framework of the Community should encompass the full range of investor-oriented activities. To this end, it is necessary to provide for the degree of harmonisation needed to offer investors a high level of protection and to allow investment firms to provide services throughout the Community, on the basis of home country supervision. In view of the preceding, Directive 93/22/EEC should be replaced by a new Directive.

(3) Due to the increasing dependence of investors on personal recommendations, it is appropriate to include the provision of investment advice as an investment service requiring authorisation.

(4) It is appropriate to include in the list of financial instruments certain commodity derivatives and others which are constituted and traded in such a manner as to give rise to regulatory issues comparable to traditional financial instruments.

(5) It is necessary to establish a comprehensive regulatory regime governing the execution of transactions in financial instruments irrespective of the trading methods used to conclude those transactions so as to ensure a high quality of execution of investor transactions and to uphold the integrity and overall efficiency of the financial system. A coherent and risk-sensitive framework for regulating the main types of order-execution arrangement currently active in the European financial marketplace should be provided for. It is necessary to recognise the emergence of a new generation of organised trading systems alongside regulated markets which should be subjected to obligations designed to preserve the efficient and orderly functioning of financial markets. With a view to
establishing a proportionate regulatory framework provision should be made for the inclusion of a new investment service which relates to the operation of an MTF.

(6) Definitions of regulated market and MTF should be introduced and closely aligned with each other to reflect the fact that they represent the same organised trading functionality. The definitions should exclude bilateral systems where an investment firm enters into every trade on own account and not as a riskless counterparty interposed between the buyer and seller. The term 'system' encompasses all those markets that are composed of a set of rules and a trading platform as well as those that only function on the basis of a set of rules. Regulated markets and MTFs are not obliged to operate a 'technical' system for matching orders. A market which is only composed of a set of rules that governs aspects related to membership, admission of instruments to trading, trading between members, reporting and, where applicable, transparency obligations is a regulated market or an MTF within the meaning of this Directive and the transactions concluded under those rules are considered to be concluded under the systems of a regulated market or an MTF. The term 'buying and selling interests' is to be understood in a broad sense and includes orders, quotes and indications of interest. The requirement that the interests be brought together in the system by means of non-discretionary rules set by the system operator means that they are brought together under the system's rules or by means of the system's protocols or internal operating procedures (including procedures embodied in computer software). The term 'non-discretionary rules' means that these rules leave the investment firm operating an MTF with no discretion as to how interests may interact. The definitions require that interests be brought together in such a way as to result in a contract, meaning that execution takes place under the system's rules or by means of the system's protocols or internal operating procedures.

[—]

(8) Persons administering their own assets and undertakings, who do not provide investment services and/or perform investment activities other than dealing on own account unless they are market makers or they deal on own account outside a regulated market or an MTF on an organised, frequent and systematic basis, by providing a system accessible to third parties in order to engage in dealings with them should not be covered by the scope of this Directive.

(9) References in the text to persons should be understood as including both natural and legal persons.

(10) Insurance or assurance undertakings the activities of which are subject to appropriate monitoring by the competent prudential-supervision authorities and which are subject to Council Directive 64/225/EEC of 25 February 1964 on the abolition of restrictions on freedom of establishment and freedom to provide services in respect of reinsurance and retrocession (6 ), First Council Directive 73/239/EEC of 24 July 1973 on the coordination of laws, regulations and administrative provisions relating to the taking up and pursuit of direct insurance other than life assurance (7 ) and Council Directive 2002/83/EC of 5 November 2002 concerning life assurance (8 ) should be excluded.

[—]

HAVE ADOPTED THIS DIRECTIVE:

[—]

Section 2

Provisions to ensure investor protection

Article 19

Conduct of business obligations when providing investment services to clients

1. Member States shall require that, when providing investment services and/or, where appropriate, ancillary services to clients, an investment firm act honestly, fairly and professionally in accordance with the best interests of its clients and comply, in particular, with the principles set out in paragraphs 2 to 8.

2. All information, including marketing communications, addressed by the investment firm to clients or potential clients shall be fair, clear and not misleading. Marketing communications shall be clearly identifiable as such.

3. Appropriate information shall be provided in a comprehensible form to clients or potential clients about:

— the investment firm and its services,
— financial instruments and proposed investment strategies; this should include appropriate guidance on and warnings of the risks associated with investments in those instruments or in respect of particular investment strategies,
— execution venues, and
— costs and associated charges

3. so that they are reasonable able to understand the nature and risks of the investment service and of the specific type of financial instrument that is being offered and, consequently, to take investment decisions on an informed basis. This information may be provided in a standardised format.

4. When providing investment advice or portfolio management the investment firm shall obtain the necessary information regarding the client's or potential client's knowledge and experience in the investment field relevant to the specific type of product or service, his financial situation and his investment objectives so as to enable the firm to recommend to the client or potential client the investment services and financial instruments that are suitable for him.

5. Member States shall ensure that investment firms, when providing investment services other than those referred to in paragraph 4, ask the client or potential client to provide information regarding his knowledge and experience in the investment field relevant to the specific type of product or service offered or demanded so as to enable the investment firm to assess whether the investment service or product envisaged is appropriate for the client.

In cases where the investment firm considers, on the basis of the information received under the previous subparagraph, that the product or service is not appropriate to the client or potential client, the investment firm shall warn the client or potential client. This warning may be provided in a standardised format.

In cases where the client or potential client elects not to provide the information referred to under the first subparagraph, or when the information provided is insufficient information regarding his knowledge and experience, the investment firm shall warn the client or potential client that such a decision will not allow the firm to determine whether the service or product envisaged is appropriate for him. This warning may be provided in a standardised format.

6. Member States shall allow investment firms when providing investment services that only consist of execution and/or the reception and transmission of client orders with or without ancillary services to provide those investment services to their clients without the need to obtain the information or make the determination provided for in paragraph 5 where all the following conditions are met:

— the services referred to in the introductory part relate to shares admitted to trading on a regulated market or in an equivalent third-country market, money market instruments, bonds or other forms of securitised debt (excluding those bonds or securitised debt that embed a derivative), UCITS and other non-complex financial instruments. A third-country market shall be considered as equivalent to a regulated market if it complies with equivalent requirements to those established under Title III. The Commission and ESMA shall publish on their websites a list of those markets that are to be considered as equivalent. That list shall be updated
periodically. ESMA shall assist the Commission in the assessment of third-country markets,
— the service is provided at the initiative of the client or potential client,
— the client or potential client has been clearly informed that in the provision of this service the investment firm is not required to assess the suitability of the instrument or service provided or offered and that therefore he does not benefit from the corresponding protection of the relevant conduct of business rules; this warning may be provided in a standardised format,
— the investment firm complies with its obligations under Article 18.
7. The investment firm shall establish a record that includes the document or documents agreed between the firm and the client that set out the rights and obligations of the parties, and the other terms on which the firm will provide services to the client. The rights and duties of the parties to the contract may be incorporated by reference to other documents or legal texts.
8. The client must receive from the investment firm adequate reports on the service provided to its clients. These reports shall include, where applicable, the costs associated with the transactions and services undertaken on behalf of the client.
9. In cases where an investment service is offered as part of a financial product which is already subject to other provisions of Community legislation or common European standards related to credit institutions and consumer credits with respect to risk assessment of clients and/or information requirements, this service shall not be additionally subject to the obligations set out in this Article.
10. In order to ensure the necessary protection of investors and the uniform application of paragraphs 1 to 6, the Commission shall adopt implementing measures to ensure that investment firms comply with the principles set out therein when providing investment or ancillary services to their clients. Those implementing measures shall take into account:
(a) the nature of the service(s) offered or provided to the client or potential client, taking into account the type, object, size and frequency of the transactions;
(b) the nature of the financial instruments being offered or considered;
(c) the retail or professional nature of the client or potential client.
The measures referred to in the first subparagraph, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).
Article 20
Provision of services through the medium of another investment firm
Member States shall allow an investment firm receiving an instruction to perform investment or ancillary services on behalf of a client through the medium of another investment firm to rely on client information transmitted by the latter firm. The investment firm which mediates the instructions will remain responsible for the completeness and accuracy of the information transmitted.
The investment firm which receives an instruction to undertake services on behalf of a client in this way shall also be able to rely on any recommendations in respect of the service or transaction that have been provided to the client by another investment firm. The investment firm which mediates the instructions will remain responsible for the appropriateness for the client of the recommendations or advice provided.
The investment firm which receives client instructions or orders through the medium of another investment firm shall remain responsible for concluding the service or transaction, based on any such information or recommendations, in accordance with the relevant provisions of this Title.
Article 21
Obligation to execute orders on terms most favourable to the client
1. Member States shall require that investment firms take all reasonable steps to obtain, when executing orders, the best possible result for their clients taking into account price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order. Nevertheless, whenever there is a specific instruction from the client the investment firm shall execute the order following the specific instruction.
2. Member States shall require investment firms to establish and implement effective arrangements for complying with paragraph 1. In particular Member States shall require investment firms to establish and implement an order execution policy to allow them to obtain, for their client orders, the best possible result in accordance with paragraph 1.
3. The order execution policy shall include, in respect of each class of instruments, information on the different venues where the investment firm executes its client orders and the factors affecting the choice of execution venue. It shall at least include those venues that enable the investment firm to obtain on a consistent basis the best possible result for the execution of client orders.
Member States shall require that investment firms provide appropriate information to their clients on their order execution policy. Member States shall require that investment firms obtain the prior consent of their clients to the execution policy.
Member States shall require that, where the order execution policy provides for the possibility that client orders may be executed outside a regulated market or an MTF, the investment firm shall, in particular, inform its clients about this possibility. Member States shall require that investment firms obtain the prior express consent of their clients before proceeding to execute their orders outside a regulated market or an MTF. Investment firms may obtain this consent either in the form of a general agreement or in respect of individual transactions.
4. Member States shall require investment firms to monitor the effectiveness of their order execution arrangements and execution policy in order to identify and, where appropriate, correct any deficiencies. In particular, they shall assess, on a regular basis, whether the execution venues included in the order execution policy provide for the best possible result for the client or whether they need to make changes to their execution arrangements. Member States shall require investment firms to notify clients of any material changes to their order execution arrangements or execution policy.
5. Member States shall require investment firms to be able to demonstrate to their clients, at their request, that they have executed their orders in accordance with the firm’s execution policy.
6. In order to ensure the protection necessary for investors, the fair and orderly functioning of markets, and to ensure the uniform application of paragraphs 1, 3 and 4, the Commission shall adopt implementing measures concerning:
(a) the criteria for determining the relative importance of the different factors that, pursuant to paragraph 1, may be taken into account for determining the best possible result taking into account the size and type of order and the retail or professional nature of the client;
(b) factors that may be taken into account by an investment firm when reviewing its execution arrangements and the circumstances under which changes to such arrangements may be appropriate. In particular, the factors for determining which venues enable investment firms to obtain on a consistent basis the best possible result for executing the client orders;
(c) the nature and extent of the information to be provided to clients on their execution policies, pursuant to paragraph 3.
The measures referred to in the first subparagraph, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).

Article 22
Client order handling rules
1. Member States shall require that investment firms authorised to execute orders on behalf of clients implement procedures and arrangements which provide for the prompt, fair and expeditious execution of client orders, relative to other client orders or the trading interests of the investment firm. These procedures or arrangements shall allow for the execution of otherwise comparable client orders in accordance with the time of their reception by the investment firm.
2. Member States shall require that, in the case of a client limit order in respect of shares admitted to trading on a regulated market which are not immediately executed under prevailing market conditions, investment firms are, unless the client expressly instructs otherwise, to take measures to facilitate the earliest possible execution of that order by making public immediately that client limit order in a manner which is easily accessible to other market participants. Member States may decide that investment firms comply with this obligation by transmitting the client limit order to a regulated market and/or MTF. Member States shall provide that the competent authorities may waive the obligation to make public a limit order that is large in scale compared with normal market size as determined under Article 44(2).
3. In order to ensure that measures for the protection of investors and fair and orderly functioning of markets take account of technical developments in financial markets, and to ensure the uniform application of paragraphs 1 and 2, the Commission shall adopt implementing measures which define:
(a) the conditions and nature of the procedures and arrangements which result in the prompt, fair and expeditious execution of client orders and the situations in which or types of transaction for which investment firms may reasonably deviate from prompt execution so as to obtain more favourable terms for clients;
(b) the different methods through which an investment firm can be deemed to have met its obligation to disclose not immediately executable client limit orders to the market.
The measures referred to in the first subparagraph, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).

Article 23
Obligations of investment firms when appointing tied agents
1. Member States may decide to allow investment firms to appoint tied agents for the purposes of promoting the services of the investment firm, soliciting business or receiving orders from clients or potential clients and transmitting them, placing financial instruments and providing advice in respect of such financial instruments and services offered by that investment firm.
2. Member States shall require that where an investment firm decides to appoint a tied agent it remains fully and unconditionally responsible for any action or omission on the part of the tied agent when acting on behalf of the firm. Member States shall require the investment firm to ensure that a tied agent discloses the capacity in which he is acting and the firm which he is representing when contacting or before dealing with any client or potential client. Member States may allow, in accordance with Article 13(6), (7) and (8), tied agents registered in their territory to handle clients’ money and/or financial instruments on behalf and under the full responsibility of the investment firm for which they are acting within their territory or, in the case of a cross-border operation, in the territory of a Member State which allows a tied agent to handle clients’ money.

Member States shall require the investment firms to monitor the activities of their tied agents so as to ensure that they continue to comply with this Directive when acting through tied agents.
3. Member States that decide to allow investment firms to appoint tied agents shall establish a public register. Tied agents shall be registered in the public register in the Member State where they are established. ESMA shall publish on its website references or hyperlinks to the public registers established under this Article by the Member States that decide to allow investment firms to appoint tied agents. Where the Member State in which the tied agent is established has decided, in accordance with paragraph 1, not to allow the investment firms authorised by their competent authorities to appoint tied agents, those tied agents shall be registered with the competent authority of the home Member State of the investment firm on whose behalf it acts.
Member States shall ensure that tied agents are only admitted to the public register if it has been established that they are of sufficiently good repute and that they possess appropriate general, commercial and professional knowledge so as to be able to communicate accurately all relevant information regarding the proposed service to the client or potential client. Member States may decide that investment firms can verify whether the tied agents which they have appointed are of sufficiently good repute and possess the knowledge as referred to in the third subparagraph.
The register shall be updated on a regular basis. It shall be publicly available for consultation.
4. Member States shall require that investment firms appointing tied agents take adequate measures in order to avoid any negative impact that the activities of the tied agent not covered by the scope of this Directive could have on the activities carried out by the tied agent on behalf of the investment firm.
Member States may allow competent authorities to collaborate with investment firms and credit institutions, their associations and other entities in registering tied agents and in monitoring compliance of tied agents with the requirements of paragraph 3. In particular, tied agents may be registered by an investment firm, credit institution or their associations and other entities under the supervision of the competent authority.
5. Member States shall require that investment firms appoint only tied agents entered in the public registers referred to in paragraph 3.
6. Member States may reinforce the requirements set out in this Article or add other requirements for tied agents registered within their jurisdiction.

Article 24
Transactions executed with eligible counterparties
1. Member States shall ensure that investment firms authorised to execute orders on behalf of clients and/or to deal on own account and/or to receive and transmit orders, may bring about or enter into transactions with eligible counterparties without being obliged to comply with the obligations under Articles 19, 21 and 22(1) in respect of those transactions or in respect of any ancillary service directly related to those transactions.
2. Member States shall recognise as eligible counterparties for the purposes of this Article investment firms, credit institutions, insurance companies, UCITS and their management companies, pension funds and their management companies, other financial institutions authorised or regulated under Community legislation or the national law of a Member State, undertakings exempted from the application of this Directive under Article 2(1)(8) and (1), national governments and their corresponding offices including public bodies that deal with public debt, central banks and supranational organisations.
Section 3
Market transparency and integrity

Article 25
Obligation to uphold integrity of markets, report transactions and maintain records
1. Without prejudice to the allocation of responsibilities for enforcing the provisions of Directive 2003/6/Eo of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) (29), Member States shall require investment firms to keep at the disposal of the competent authority, for at least 5 years, the relevant data relating to all transactions in financial instruments which they have carried out, whether on own account or on behalf of a client. In the case of transactions carried out on behalf of clients, the records shall contain all the information and details of the identity of the client, and the information required under Directive 2005/60/EC.
2. ESMA may request access to that information in accordance with the procedure and under the conditions set out in Article 35 of Regulation (EU) No 1095/2010.
3. Member States shall require investment firms which execute transactions in any financial instruments admitted to trading on a regulated market to report details of such transactions to the competent authority as quickly as possible, and no later than the close of the following working day. This obligation shall apply whether or not such transactions were carried out on a regulated market.

The competent authorities shall, in accordance with Article 58, establish the necessary arrangements in order to ensure that the competent authority of the most relevant market in terms of liquidity for those financial instruments also receives this information.
4. The reports shall, in particular, include details of the names and numbers of the instruments bought or sold, the quantity, the dates and times of execution and the transaction prices and means of identifying the investment firms concerned.
5. Member States shall provide for the reports to be made to the competent authority either by the investment firm itself, a third party acting on its behalf or by a trade-matching or reporting system approved by the competent authority or by the regulated market or MTF through whose systems the transaction was completed. In cases where transactions are reported directly to the competent authority by a regulated market, an MTF, or a trade-matching or reporting system approved by the competent authority, the obligation on the investment firm laid down in paragraph 3 may be waived.
6. When, in accordance with Article 32(7), reports provided for under this Article are transmitted to the competent authority of the host Member State, it shall transmit this information to the competent authorities of the home Member State of the investment firm, unless they decide that they do not want to receive this information.
7. In order to ensure that measures for the protection of market integrity are modified to take account of technical developments in financial markets, and to ensure the uniform application of paragraphs 1 to 5, the Commission may adopt implementing measures which define the methods and arrangements for reporting financial transactions, the form and content of these reports and the criteria for defining a relevant market in accordance with paragraph 3. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).

Article 26
Monitoring of compliance with the rules of the MTF and with other legal obligations
1. Member States shall require that investment firms and market operators operating an MTF establish and maintain effective arrangements and procedures, relevant to the MTF, for the regular monitoring of the compliance by its users with its rules. Investment firms and market operators operating an MTF shall monitor the transactions undertaken by their users under their systems in order to identify breaches of those rules, disorderly trading conditions or conduct that may involve market abuse.
2. Member States shall require investment firms and market operators operating an MTF to report significant breaches of its rules or disorderly trading conditions or conduct that may involve market abuse to the competent authority. Member States shall also require investment firms and market operators operating an MTF to supply the relevant information without delay to the authority competent for the investigation and prosecution of market abuse and to provide full assistance to the latter in investigating and prosecuting market abuse occurring on or through its systems.

[...]
States shall provide for this information to be made available to the public on reasonable commercial terms and on a continuous basis during normal trading hours.

2. Member States shall provide for the competent authorities to be able to waive the obligation for investment firms or market operators operating an MTF to make public the information referred to in paragraph 1 based on the market model or the type and size of orders in the cases defined in accordance with paragraph 3. In particular, the competent authorities shall be able to waive the obligation in respect of transactions that are large in scale compared with normal market size for the share or type of share in question.

3. In order to ensure the uniform application of paragraphs 1 and 2, the Commission shall adopt implementing measures as regards:

(a) the range of bid and offers or designated market-maker quotes, and the depth of trading interest at those prices, to be made public;

(b) the size or type of orders for which pre-trade disclosure may be waived under paragraph 2;

(c) the market model for which pre-trade disclosure may be waived under paragraph 2 and in particular, the applicability of the obligation to trading methods operated by an MTF which conclude transactions under their rules by reference to prices established outside the systems of the MTF or by periodic auction.

Except where justified by the specific nature of the MTF, the content of these implementing measures shall be equal to that of the implementing measures provided for in Article 44 for regulated markets.

The measures referred to in the first subparagraph, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).

Article 30

Post-trade transparency requirements for MTFs

1. Member States shall, at least, require that investment firms and market operators operating an MTF make public the price, volume and time of the transactions executed under its systems in respect of shares which are admitted to trading on a regulated market. Member States shall require that details of all such transactions be made public, on a reasonable commercial basis, as close to real-time as possible. This requirement shall not apply to details of trades executed on an MTF that are made public under the systems of a regulated market.

2. Member States shall provide that the competent authority may authorise investment firms or market operators operating an MTF to provide for deferred publication of the details of transactions based on their type or size. In particular, the competent authorities may authorise the deferred publication in respect of transactions that are large in scale compared with the normal market size for that share or that class of shares. Member States shall require MTFs to obtain the competent authority’s prior approval to proposed arrangements for deferred trade-publication, and shall require that these arrangements be clearly disclosed to market participants and the investing public.

3. In order to provide for the efficient and orderly functioning of financial markets, and to ensure the uniform application of paragraphs 1 and 2, the Commission shall adopt implementing measures in respect of:

(a) the scope and content of the information to be made available to the public;

(b) the conditions under which investment firms or market operators operating an MTF may provide for deferred publication of trades and the criteria to be applied when deciding the transactions for which, due to their size or the type of share involved, deferred publication is allowed.

Except where justified by the specific nature of the MTF, the content of these implementing measures shall be equal to that of the implementing measures provided for in Article 45 for regulated markets.

The measures referred to in the first subparagraph, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 64(2).

CHAPTER III

RIGHTS OF INVESTMENT FIRMS

Article 31

Freedom to provide investment services and activities

1. Member States shall ensure that any investment firm authorised and supervised by the competent authorities of another Member State in accordance with this Directive, and in respect of credit institutions in accordance with Directive 2000/12/EC, may freely perform investment services and/or activities as well as ancillary services within their territories, provided that such services and activities are covered by its authorisation. Ancillary services may only be provided together with an investment service and/or activity.

Member States shall not impose any additional requirements on such an investment firm or credit institution in respect of the matters covered by this Directive.

2. Any investment firm wishing to provide services or activities within the territory of another Member State for the first time, or which wishes to change the range of services or activities so provided, shall communicate the following information to the competent authorities of its home Member State:

(a) the Member State in which it intends to operate;

(b) a programme of operations stating in particular the investment services and/or activities as well as ancillary services which it intends to perform and whether it intends to use tied agents in the territory of the Member States in which it intends to provide services.

3. The competent authority of the home Member State shall, within one month of receiving the information, forward it to the competent authority of the host Member State designated as contact point in accordance with Article 56(1). The investment firm may then start to provide the investment service or services concerned in the host Member State.

4. In the event of a change in any of the particulars communicated in accordance with paragraph 2, an investment firm shall give written notice of that change to the competent authority of the home Member State at least one month before implementing the change. The competent authority of the home Member State shall inform the competent authority of the host Member State of those changes.

5. Member States shall, without further legal or administrative requirement, allow investment firms and market operators operating MTFs from other Member States to provide appropriate arrangements on their territory so as to facilitate access to and use of their systems by remote users or participants established in their territory.

6. The investment firm or the market operator that operates an MTF shall communicate to the competent authority of its home Member State the MTF in which it intends to provide such arrangements. The competent authority of the home Member State of the MTF shall communicate, within one month, this information to the Member State in which the MTF intends to provide such arrangements.

7. The competent authority of the home Member State of the MTF shall, on the request of the competent authority of the host Member State of the MTF and within a reasonable delay, communicate the identity of the members or participants of the MTF established in that Member State.

In order to ensure consistent harmonisation of this Article, ESMA may develop draft regulatory technical standards to
specify the information to be notified in accordance with paragraphs 2, 4 and 6.

7. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.

[...]

Article 32
Establishment of a branch
1. Member States shall ensure that investment services and/or activities as well as ancillary services may be provided within their territories in accordance with this Directive and Directive 2000/12/EC through the establishment of a branch provided that those services and activities are covered by the authorisation granted to the investment firm or the credit institution in the home Member State. Ancillary services may only be provided together with an investment service and/or activity.

Member States shall not impose any additional requirements save those allowed under paragraph 7, on the organisation and operation of the branch in respect of the matters covered by this Directive.

2. Member States shall require any investment firm wishing to establish a branch within the territory of another Member State first to notify the competent authority of its home Member State and to provide it with the following information:
   (a) the Member States within the territory of which it plans to establish a branch;
   (b) a programme of operations setting out inter alia the investment services and/or activities as well as the ancillary services to be offered and the organisational structure of the branch and indicating whether the branch intends to use tied agents;
   (c) the address in the host Member State from which documents may be obtained;
   (d) the names of those responsible for the management of the branch.

In cases where an investment firm uses a tied agent established in a Member State outside its home Member State, such tied agent shall be assimilated to the branch and shall be subject to the provisions of this Directive relating to branches.

3. Unless the competent authority of the home Member State has reason to doubt the adequacy of the administrative structure or the financial situation of an investment firm, taking into account the activities envisaged, it shall, within three months of receiving all the information, communicate that information to the competent authority of the host Member State designated as contact point in accordance with Article 56(1) and inform the investment firm concerned accordingly.

4. In addition to the information referred to in paragraph 2, the competent authority of the home Member State shall communicate details of the accredited compensation scheme of which the investment firm is a member in accordance with Directive 97/9/EC to the competent authority of the host Member State. In the event of a change in the particulars, the competent authority of the home Member State shall inform the competent authority of the host Member State accordingly.

5. Where the competent authority of the home Member State refuses to communicate the information to the competent authority of the host Member State, it shall give reasons for its refusal to the investment firm concerned within three months of receiving all the information.

6. On receipt of a communication from the competent authority of the host Member State, or failing such communication from the latter at the latest after two months from the date of transmission of the communication by the competent authority of the home Member State, the branch may be established and commence business.

7. The competent authority of the Member State in which the branch is located shall assume responsibility for ensuring that the services provided by the branch within its territory comply with the obligations laid down in Articles 19, 21, 22, 25, 27 and 28 and in measures adopted pursuant thereto.

The competent authority of the Member State in which the branch is located shall have the right to examine branch arrangements and to request such changes as are strictly needed to enable the competent authority to enforce the obligations under Articles 19, 21, 22, 25, 27 and 28 and measures adopted pursuant thereto with respect to the services and/or activities provided by the branch within its territory.

8. Each Member State shall provide that, where an investment firm authorised in another Member State has established a branch within its territory, the competent authority of the home Member State of the investment firm, in the exercise of its responsibilities and after informing the competent authority of the host Member State, may carry out on-site inspections in that branch.

9. In the event of a change in any of the information communicated in accordance with paragraph 2, an investment firm shall give written notice of that change to the competent authority of the home Member State at least one month before implementing the change. The competent authority of the host Member State shall also be informed of that change by the competent authority of the home Member State.

10. In order to ensure consistent harmonisation of this Article, ESMA may develop draft regulatory technical standards to specify the information to be notified in accordance with paragraphs 2, 4 and 9.

[...]

Article 33
Access to regulated markets
1. Member States shall require that investment firms from other Member States which are authorised to execute client orders or to deal on own account have the right of membership or have access to regulated markets established in their territory by means of any of the following arrangements:
   (a) directly, by setting up branches in the host Member States;
   (b) by becoming remote members of or having remote access to the regulated market without having to be established in the home Member State of the regulated market, where the trading procedures and systems of the market in question do not require a physical presence for conclusion of transactions on the market.

2. Member States shall not impose any additional regulatory or administrative requirements, in respect of matters covered by this Directive, on investment firms exercising the right conferred by paragraph 1.

Article 34
Access to central counterparty, clearing and settlement facilities and right to designate settlement system
1. Member States shall require that investment firms from other Member States have the right of access to central counterparty, clearing and settlement systems in their territory for the purposes of finalising or arranging the finalisation of transactions in financial instruments.

Member States shall require that access of those investment firms to such facilities be subject to the same non-discriminatory, transparent and objective criteria as apply to local participants. Member States shall not restrict the use of those facilities to the clearing and settlement of transactions in financial instruments undertaken on a regulated market or MTF in their territory.

2. Member States shall require that regulated markets in their territory offer all their members or participants the right to designate the system for the settlement of transactions in
financial instruments undertaken on that regulated market, subject to:
(a) such links and arrangements between the designated settlement system and any other system or facility as are necessary to ensure the efficient and economic settlement of the transaction in question; and
(b) agreement by the competent authority responsible for the supervision of the regulated market that technical conditions for settlement of transactions concluded on the regulated market through a settlement system other than that designated by the regulated market are such as to allow the smooth and orderly functioning of financial markets.

This assessment of the competent authority of the regulated market shall be without prejudice to the competencies of the national central banks as overseers of settlement systems or other supervisory authorities on such systems. The competent authority shall take into account the oversight/supervision already exercised by those institutions in order to avoid undue duplication of control.

3. The rights of investment firms under paragraphs 1 and 2 shall be without prejudice to the right of operators of central counterparty, clearing or securities settlement systems to refuse on legitimate commercial grounds to make the requested services available.

Amended by:


Corrected by:

| C1 | Corrigendum, OJ L 045, 16.2.2005, p. 18 (2004/39) |


T'HE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 47(2), first and third sentences, and Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the European Central Bank (2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

(2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to avoid Member States' adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy, Community action in this area is necessary.

(3) In order to facilitate their criminal activities, money launderers and terrorist financiers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Community level.

(4) In order to respond to these concerns in the field of money laundering, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (4) was adopted. It required Member States to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities.

(5) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even Community level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the Community in this field should therefore be consistent with other action undertaken in other international fora. The Community action should continue to take particular account of the Recommendations of the Financial Action Task Force (hereinafter referred to as the FATF), which constitutes the foremost international body active in the fight against money laundering and terrorist financing. Since the FATF Recommendations were substantially revised and expanded in 2003, this Directive should be in line with that new international standard.

(8) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes.

(10) The institutions and persons covered by this Directive should, in conformity with this Directive, identify and verify the identity of the beneficial owner. To fulfil this requirement, it should be left to those institutions and persons whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

(11) Credit agreements in which the credit account serves exclusively to settle the loan and the repayment of the loan is effected from an account which was opened in the name of the customer with a credit institution covered by this Directive pursuant to Article 8(1)(a) to (c) should generally be considered as an example of types of less risky transactions.

(12) To the extent that the providers of the property of a legal entity or arrangement have significant control over the use of the property they should be identified as a beneficial owner.

(13) Trust relationships are widely used in commercial products as an internationally recognised feature of the comprehensively supervised wholesale financial markets. An obligation to identify the beneficial owner does not arise from the fact alone that there is a trust relationship in this particular case.

(14) This Directive should also apply to those institutions and persons covered hereunder which are performed on the Internet.

(15) As the tightening of controls in the financial sector has prompted money launderers and terrorist financiers to seek alternative methods for concealing the origin of the proceeds of crime and as such channels can be used for terrorist financing, the anti-money laundering and anti-terrorist financing obligations should cover life insurance intermediaries and trust and company service providers.

(18) The use of large cash payments has repeatedly proven to be very vulnerable to money laundering and terrorist financing. Therefore, in those Member States that allow cash payments above the established threshold, all natural or legal persons trading in goods by way of business should be covered by this Directive when accepting such cash payments. Dealers in high-value goods, such as precious stones or metals, or works of art, and auctioneers are in any event covered by this Directive to the extent that payments to them are made in cash in an amount of EUR 15 000 or more. To ensure effective monitoring of compliance with this Directive by that potentially wide group of institutions and persons, Member States may focus their monitoring activities in particular on those natural and legal persons trading in goods that are exposed to a relatively high risk of money laundering or terrorist financing, in accordance with the principle of risk-based supervision. In view of the different situations in the various Member States, Member States may decide to adopt stricter provisions, in order to properly address the risk involved with large cash payments.

(20) Where independent members of professions providing legal advice which are legally recognised and controlled,
such as lawyers, are ascertaining the legal position of a client or representing a client in legal proceedings, it would not be appropriate under this Directive to put those legal professionals in respect of these activities under an obligation to report suspicions of money laundering or terrorist financing. There must be an exemption from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position for a client. Thus, legal advice shall remain subject to the obligation of professional secrecy unless the legal counsel is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.

[...]

(22) It should be recognised that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be introduced into Community legislation that simplified customer due diligence is allowed in appropriate cases.

(23) The derogation concerning the identification of beneficial owners of pooled accounts held by notaries or other independent legal professionals should be without prejudice to the obligations that those notaries or other independent legal professionals have pursuant to this Directive. Those obligations include the need for such notaries or other independent legal professionals themselves to identify the beneficial owners of the pooled accounts held by them.

(24) Equally, Community legislation should recognise that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

[...]

(27) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers to be introduced whose identification has been carried out elsewhere. Where an institution or person covered by this Directive relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the institution to whom the customer is introduced. The third party, or introducer, also retains his own responsibility for all the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

(28) In the case of agency or outsourcing relationships on a contractual basis between institutions or persons covered by this Directive and external natural or legal persons not covered hereby, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the institutions or persons covered by this Directive, may only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the institution or person covered hereby.

(29) Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfettered to FIUs, allowing them to conduct their business properly, including international cooperation with other FIUs.

(30) By way of derogation from the general prohibition on executing suspicious transactions, the institutions and persons covered by this Directive may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(31) Where a Member State decides to make use of the exemptions provided for in Article 23(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.

(32) There has been a number of cases of employees who report their suspicions of money laundering being subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect employees from such threats or hostile action.

(33) Disclosure of information as referred to in Article 28 should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ( 6 ). Moreover, Article 28 cannot interfere with national data protection and professional secrecy legislation.

(34) Persons who merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.

(35) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where community credit and financial institutions have branches and subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within an institution or group of institutions, apply the Community standard or notify the competent authorities of the home Member State if this application is impossible.

(36) It is important that credit and financial institutions should be able to respond rapidly to requests for information on whether they maintain business relationships with named persons. For the purpose of identifying such business relationships in order to be able to provide that information quickly, credit and financial institutions should have effective systems in place which are commensurate with the size and nature of their business. In particular it would be appropriate for credit institutions and larger financial institutions to have electronic systems at their disposal. This provision is of particular importance in the context of procedures leading to measures such as the freezing or seizing of assets (including terrorist assets), pursuant to applicable national or Community legislation with a view to combating terrorism.
(39) When registering or licensing a currency exchange office, a trust and company service provider or a casino nationally, competent authorities should ensure that the persons who effectively direct or will direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should be established in conformity with national law. As a minimum, such criteria should reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(40) Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between FIUs as referred to in Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (7), including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent. To that end, the Commission should lend such assistance as may be needed to facilitate such coordination, including financial assistance.

(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive penalties in national law for failure to respect the national provisions adopted pursuant to this Directive. Provision should be made for penalties in respect of natural and legal persons. Since legal persons are often involved in complex money laundering or terrorist financing operations, sanctions should also be adjusted in line with the activity carried on by legal persons.

[...]

(48) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.

2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (9).

5. Knowledge, intent or purpose required as an element of the activities mentioned in paragraphs 2 and 4 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) casinos.

2. Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or terrorist financing occurring do not fall within the scope of Article 3(1) or (2).

Article 3

For the purposes of this Directive the following definitions shall apply:

(1) 'credit institution' means a credit institution, as defined in the first subparagraph of Article 1(1) of Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions (10), including branches within the meaning of Article 1(3) of that Directive located in the Community of credit institutions having their head offices inside or outside the Community;

(2) 'financial institution' means:

(a) an undertaking, other than a credit institution, which carries out one or more of the operations included in points 2 to 12 and points 14 and 15 of Annex I to Directive 2006/43/EC, including the activities of currency exchange offices (bureaux de change);

(b) an insurance company duly authorised in accordance with Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance (11), insofar as it carries out activities covered by that Directive;

(c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (12);

(3) the following legal or natural persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) casinos.
(d) a collective investment undertaking marketing its units or shares;
(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation (13), with the exception of intermediaries as mentioned in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;
(f) branches, when located in the Community, of financial institutions as referred to in points (a) to (e), whose head offices are outside the Community;

(3) 'property' means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of a serious crime;

(5) 'serious crimes' means, at least:
(a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA;
(b) any of the offences defined in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (14);
(d) fraud, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities’ Financial Interests (15);
(e) corruption;
(f) all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

(6) 'beneficial owner' means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5
The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.

CHAPTER II
CUSTOMER DUE DILIGENCE

SECTION 1
General provisions

Article 6
Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. By way of derogation from Article 9(6), Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be made the subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

Article 7
The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:
(a) when establishing a business relationship;
(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 8
1. Customer due diligence measures shall comprise:
(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
(b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;
(c) obtaining information on the purpose and intended nature of the business relationship;
(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

2. The institutions and persons covered by this Directive shall apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be
able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Article 9
1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction.
2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.
3. By way of derogation from paragraphs 1 and 2, Member States may, in relation to life insurance business, allow the verification of the identity of the beneficiary under the policy to take place after the business relationship has been established. In that case, verification shall take place at or before the time of payout or at or before the time the beneficiary intends to exercise rights vested under the policy.
4. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the aforementioned provisions is obtained.
5. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 8(1), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider making a report to the financial intelligence unit (FIU) in accordance with Article 22 in relation to the customer.

Member States shall not be obliged to apply the previous subparagraph in situations when notaries, independent legal professionals, auditors, external accountants and tax advisors are in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.
6. Member States shall require that institutions and persons covered by this Directive apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

Article 10
1. Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2 000 or more.
2. Casinos subject to State supervision shall be deemed in any event to have satisfied the customer due diligence requirements if they register, identify and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased.

SECTION 2

Simplified customer due diligence

Article 11
1. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), the institutions and persons covered by this Directive shall not be subject to the requirements provided for in those Articles where the customer is a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements.
2. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:
(a) listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;
(b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering and terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts;
(c) domestic public authorities,
2. or in respect of any other customer representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).
3. In the cases mentioned in paragraphs 1 and 2, institutions and persons covered by this Directive shall in any case gather sufficient information to establish if the customer qualifies for an exemption as mentioned in these paragraphs.
4. The Member States shall inform each other, the European Supervisory Authority (European Banking Authority) (hereinafter "EBA"), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council (16), the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (hereinafter "EIOPA"), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council (17), and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter "ESMA"), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council (18) (collectively, the "ESA") to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010, and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 1 or 2 or in other situations which meet the technical criteria established in accordance with Article 40(1)(b).
5. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:
(a) life insurance policies where the annual premium is no more than EUR 1 000 or the single premium is no more than EUR 2 500;
(b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;
(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
(d) electronic money, as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (19) where, if it is not possible to recharge, the maximum amount stored electronically in the device is no more than EUR 250, or where, if it is possible to recharge, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR
1 000 or more is redeemed in that same calendar year upon the electronic money holder’s request in accordance with Article 11 of Directive 2009/10/EC. As regards national payment transactions, Member States or their competent authorities may increase the amount of EUR 250 referred to in this point to a ceiling of EUR 500.

5. or in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

Article 12

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the institutions and persons covered by this Directive from applying simplified due diligence to credit and financial institutions or listed companies from the third country concerned or other entities following from situations which meet the technical criteria established in accordance with Article 40(1)(b).

SECTION 3

Enhanced customer due diligence

Article 13

1. Member States shall require the institutions and persons covered by this Directive to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in Articles 7, 8 and 9(6), in situations which by their nature can present a higher risk of money laundering or terrorist financing, and at least in the situations set out in paragraphs 2, 3, 4 and in other situations representing a high risk of money laundering or terrorist financing which meet the technical criteria established in accordance with Article 40(1)(b).

2. Where the customer has not been physically present for identification purposes, Member States shall require those institutions and persons to take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(a) ensuring that the customer’s identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by this Directive;

(c) ensuring that the first payment of the operations is carried out through an account opened in the customer’s name with a credit institution.

3. In respect of cross-frontier correspondent banking relationships with correspondent institutions from third countries, Member States shall require those credit institutions to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution’s anti-money laundering and anti-terrorist financing controls;

(c) obtain approval from senior management before establishing new correspondent banking relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

4. In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, Member States shall require those institutions and persons covered by this Directive to:

(a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;

(b) have senior management approval for establishing business relationships with such customers;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(d) conduct enhanced ongoing monitoring of the business relationship.

5. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

6. Member States shall ensure that the institutions and persons covered by this Directive pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

SECTION 4

Performance by third parties

Article 14

Member States may permit the institutions and persons covered by this Directive to rely on third parties to meet the requirements laid down in Article 8(1)(a) to (c). However, the ultimate responsibility for meeting those requirements shall remain with the institution or person covered by this Directive which relies on the third party.

Article 15

1. Where a Member State permits credit and financial institutions referred to in Article 2(1)(1) or (2) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit institutions and persons referred to in Article 2(1) situated in its territory to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by an institution referred to in Article 2(1)(1) or (2) in another Member State, with the exception of currency exchange offices and payment institutions as defined in Article 4(4) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (20), which mainly provide the payment service listed in point 6 of the Annex to that Directive, including natural and legal persons benefiting from a waiver under Article 26 of that Directive, and meeting the requirements laid down in Articles 16 and 18 of this Directive, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

2. Where a Member State permits currency exchange offices referred to in Article 3(2)(a) and payment institutions as defined in Article 4(4) of Directive 2007/64/EC, which mainly provide the payment service listed in point 6 of the Annex to that Directive, situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14 of this Directive, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by the same category of institution in another Member State and meeting the requirements laid down in Articles 16 and 18 of this Directive, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.
3. Where a Member State permits persons referred to in Article 2(1)(3)(a) to (c) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 2(1)(3)(a) to (c), carried out in accordance with this Directive by a person referred to in Article 2(1)(3)(a) to (c) in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

Article 16
1. For the purposes of this Section, ‘third parties’ shall mean institutions and persons who are listed in Article 2, or equivalent institutions and persons situated in a third country, who meet the following requirements:
   (a) they are subject to mandatory professional registration, recognised by law;
   (b) they apply customer due diligence requirements and record keeping requirements as laid down or equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter V, or they are situated in a third country which imposes equivalent requirements to those laid down in this Directive.
2. The Member States shall inform each other, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, and the Commission of cases where they consider that a third country meets the conditions laid down in paragraph 1(b).

Article 17
Where the Commission adopts a decision pursuant to Article 40(4), Member States shall prohibit the institutions and persons covered by this Directive from relying on third parties from the third country concerned to meet the requirements laid down in Article 8(1)(a) to (c).

Article 18
1. Third parties shall make information requested in accordance with the requirements laid down in Article 8(1)(a) to (c) immediately available to the institution or person covered by this Directive to which the customer is being referred.
2. Relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on request, by the third party to the institution or person covered by this Directive to which the customer is being referred.

Article 19
This Section shall not apply to outsourcing or agency arrangements where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the institution or person covered by this Directive.

CHAPTER III
REPORTING OBLIGATIONS

SECTION 1
General provisions

Article 20
Member States shall require that the institutions and persons covered by this Directive pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Article 21
1. Each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing.
2. That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.
3. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.

Article 22
1. Member States shall require the institutions and persons covered by this Directive, and where applicable their directors and employees, to cooperate fully:
   (a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted;
   (b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.
2. The information referred to in paragraph 1 shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 34 shall normally forward the information.

Article 23
1. By way of derogation from Article 22(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a) and (b), designate an appropriate self-regulatory body of the profession concerned as the authority to be informed in the first instance in place of the FIU. Without prejudice to paragraph 2, the designated self-regulatory body shall in such cases forward the information to the FIU promptly and unfiltered.
2. Member States shall not be obliged to apply the obligations laid down in Article 22(1) to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 24
1. Member States shall require the institutions and persons covered by this Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 22(1)(a). In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.
2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering
or terrorist financing operation, the institutions and persons concerned shall inform the FIU immediately afterwards.

Article 25:
1. Member States shall ensure that if, in the course of inspections carried out in the institutions and persons covered by this Directive by the competent authorities referred to in Article 37, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 26:
The disclosure in good faith as foreseen in Articles 22(1) and 23 by an institution or person covered by this Directive or by an employee or director of such an institution or person of the information referred to in Articles 22 and 23 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the institution or person or its directors or employees in liability of any kind.

Article 27:
Member States shall take all appropriate measures in order to protect employees of the institutions or persons covered by this Directive who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

SECTION 2
Prohibition of disclosure

Article 28:
1. The institutions and persons covered by this Directive and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 22 and 23 or that a money laundering or terrorist financing investigation is being or may be carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities referred to in Article 37, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries provided that they meet the conditions laid down in Article 11(1), belonging to the same group as defined by Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate (21).

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a network. For the purposes of this Article, a ‘network’ means the larger structure to which the person belongs and which shares common ownership, managements or compliance control.

5. For institutions or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of the paragraph 1.

7. The Member States shall inform each other, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 3, 4 or 5.

Article 29:
Where the Commission adopts a decision pursuant to Article 49(4), the Member States shall prohibit the disclosure between institutions and persons covered by this Directive and institutions and persons from the third country concerned.

CHAPTER IV
RECORD KEEPING AND STATISTICAL DATA

Article 30:
Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law:
(a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended;
(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

Article 31:
1. Member States shall require the credit and financial institutions covered by this Directive to apply, where applicable, in their branches and majority-owned subsidiaries located in third countries measures at least equivalent to those laid down in this Directive with regard to customer due diligence and record keeping.

Where the legislation of the third country does not permit application of such equivalent measures, the Member States shall require the credit and financial institutions concerned to inform the competent authorities of the relevant home Member State accordingly.

2. The Member States, the ESA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 and the Commission shall inform each other of cases where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1 and coordinated action could be taken to pursue a solution.

3. Member States shall require that, where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1, credit or financial institutions take additional...
measures to effectively handle the risk of money laundering or terrorist financing.

[...]

Article 32
Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

Article 33
1. Member States shall ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.
2. Such statistics shall as a minimum cover the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and indicate on an annual basis the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and how much property has been frozen, seized or confiscated.
3. Member States shall ensure that a consolidated review of these statistical reports is published.

SECTION 2
Supervision

Article 36
1. Member States shall provide that currency exchange offices and trust and company service providers shall be licensed or registered and casinos be licensed in order to operate their business legally.
2. Member States shall require competent authorities to refuse licensing or registration of the entities referred to in paragraph 1 if they are not satisfied that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.

SECTION 3
Cooperation

Article 37a
2. The competent authorities shall provide the ESA with all information necessary to carry out their duties under this Directive and under Regulation (EU) No 1093/2010, Regulation (EU) No 1094/2010 and Regulation (EU) No 1095/2010, respectively.

Article 38
The Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community.

SECTION 4
Penalties

Article 39
1. Member States shall ensure that natural and legal persons covered by this Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive.
2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure, in conformity with their national law, that the appropriate administrative measures can be taken or administrative sanctions can be imposed against credit and financial institutions for infringements of the national provisions adopted pursuant to this Directive. Member States shall ensure that these measures or sanctions are effective, proportionate and dissuasive.
3. In the case of legal persons, Member States shall ensure that at least they can be held liable for infringements referred to in paragraph 1 which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:
   (a) a power of representation of the legal person;
   (b) an authority to take decisions on behalf of the legal person, or
   (c) an authority to exercise control within the legal person.
4. In addition to the cases already provided for in paragraph 3, Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 3 has made possible the commission of the infringements referred to in paragraph 1 for the benefit of a legal person by a person under its authority.

CHAPTER VI
DELEGATED ACTS AND IMPLEMENTING MEASURES

Article 40
1. In order to take account of technical developments in the fight against money laundering and terrorist financing and to specify the requirements laid down in this Directive, the Commission may, adopt the following measures:

[...]

CHAPTER VII
FINAL PROVISIONS

Article 45
1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 15 December 2007. They shall forthwith communicate to the Commission the text of those provisions together with a table showing how the provisions of this Directive correspond to the national provisions adopted.

[...]

Amended by:

Official Journal

<table>
<thead>
<tr>
<th>No</th>
<th>page</th>
<th>date</th>
</tr>
</thead>
</table>
Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) In accordance with Article 26(2) of the Treaty on the Functioning of the European Union (TFEU), the internal market is to comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured. Fragmentation of the internal market is detrimental to competitiveness, growth and job creation within the Union. Eliminating direct and indirect obstacles to the proper functioning of the internal market is essential for its completion. Union action with respect to the internal market in the retail financial services sector has already substantially contributed to developing cross-border activity of payment service providers, improving consumer choice and increasing the quality and transparency of the offers.

(2) In this respect, Directive 2007/64/EC of the European Parliament and of the Council (4) established basic transparency requirements for fees charged by payment service providers in relation to services offered on payment accounts. This has substantially facilitated the activity of payment service providers, creating uniform rules with respect to the provision of payment services and the information to be provided, reduced the administrative burden and generated cost savings for payment service providers.

(3) The smooth functioning of the internal market and the development of a modern, socially inclusive economy increasingly depends on the universal provision of payment services. Any new legislation in this regard must be part of a smart economic strategy for the Union, which must effectively take into account the needs of more vulnerable consumers.

(4) However, as indicated by the European Parliament in its resolution of 4 July 2012 with recommendations to the Commission on Access to Basic Banking Services, more must be done to improve and develop the internal market for retail banking. Currently, the lack of transparency and comparability of fees as well as the difficulties in switching payment accounts still create barriers to the deployment of a fully integrated market contributing to low competition in the retail banking sector. Those problems must be tackled and high-quality standards must be achieved.

(5) The current conditions of the internal market could deter payment service providers from exercising their freedom to establish or to provide services within the Union because of the difficulty in attracting customers when entering a new market. Entering new markets often entails large investment. Such investment is only justified if the provider foresees sufficient opportunities and a corresponding demand from consumers. The low level of mobility of consumers with respect to retail financial services is in a large extent due to the lack of transparency and comparability as regards the fees and services on offer, as well as difficulties in relation to the switching of payment accounts. Those factors also stifle demand. This is particularly true in the cross-border context.

(6) Moreover, significant barriers to the completion of the internal market in the area of payment accounts may be created by the fragmentation of existing national regulatory frameworks. Existing provisions at national level with respect to payment accounts, and particularly with respect to the comparability of fees and payment account switching, diverge. For switching, the lack of uniform binding measures at Union level has led to divergent practices and measures at national level. Those differences are even more marked in the area of comparability of fees, where no measures, even of a self-regulatory nature, exist at Union level. Should those differences become more significant in the future, as payment service providers tend to tailor their practices to national markets, this would raise the cost of operating across borders relative to the costs faced by domestic providers and would therefore make the pursuit of business on a cross-border basis less attractive. Cross-border activity in the internal market is hampered by obstacles to consumers opening a payment account abroad. Existing restrictive eligibility criteria may prevent Union citizens from moving freely within the Union. Providing all consumers with access to a payment account will permit their participation in the internal market and allow them to reap the benefits of the internal market.

(7) Moreover, since some prospective customers do not open payment accounts, either because they are denied them or because they are not offered adequate products, the potential demand for payment account services in the Union is currently not fully exploited. Wider consumer participation in the internal market would further incentivise payment service providers to enter new markets. Also, creating the conditions to allow all consumers to access a payment account is a necessary means of fostering their participation in the internal market and of allowing them to reap the benefits of the internal market has brought about.

(8) Transparency and comparability of fees were considered at Union level in a self-regulatory initiative, initiated by the banking industry. However, no final agreement was reached on that initiative. As regards switching, the common principles established in 2008 by the European Banking Industry Committee provide a model mechanism for switching between payment accounts offered by banks located in the same Member State. However, given their non-binding nature, those common principles have been applied in an inconsistent manner throughout the Union and with ineffective results. Moreover, the common principles address payment account switching at national level only and do not address cross-border switching. For switching, the Commission has established Commission Recommendation 2008/442/EU (5) which provides a cross-border context.

(9) In order to support effective and smooth financial mobility in the long term, it is vital to establish a uniform set of rules to tackle the issue of low customer mobility, and in particular to improve comparison of payment account services and fees and
to incentivise payment account switching, as well as to avoid discrimination on the basis of residency against consumers who intend to open and use a payment account on a cross-border basis. Moreover, it is essential to adopt adequate measures to foster consumers’ participation in the payment accounts market. These measures will incentivise payment service providers in the internal market and ensure a level playing field, thereby strengthening competition and the efficient allocation of resources within the Union’s financial retail market to the benefit of businesses and consumers. Also, transparent fee information, when combined with the right of access to a payment account with basic features, will allow Union citizens to move and shop around more easily within the Union, thereby benefitting from a fully functioning internal market in the area of retail financial services, and will contribute to the further development of the internal market.

(11) This Directive should not preclude Member States from retaining or adopting more stringent provisions in order to protect consumers, provided that such provisions are consistent with their obligations under Union law and this Directive.

(13) Since a payment account with basic features is a type of payment account for the purposes of this Directive, the provisions in respect of transparency and switching should also apply to other payment accounts.

(14) The definitions contained in this Directive should be aligned as far as possible with those contained in other Union legislative acts, and in particular with those contained in Directive 2007/64/EC and in Regulation (EU) No 260/2012 of the European Parliament and of the Council (6).

(15) It is vital for consumers to be able to understand fees so that they can compare offers from different payment service providers and make informed decisions as to which payment account is most suitable for their needs. Comparison between fees cannot be made where payment service providers use different terminology for the same services and provide information in different formats. Standardised terminology, coupled with targeted fee information presented in a consistent format covering the most representative services linked to payment accounts, can help consumers to both understand and compare fees.

(16) Consumers would benefit most from information that is concise, standardised and easy to compare between different payment service providers. The tools made available to consumers to compare payment account offers would not have a positive impact if the time invested in going through lengthy lists of fees for different offers outweighed the benefit of choosing the offer that represents the best value. Those tools should be multifold and consumer testing should be conducted. At this stage, fee terminology should only be standardised for the most representative terms and definitions within Member States in order to avoid the risk of excessive information and to facilitate swift implementation.

(17) The fee terminology should be determined by Member States, allowing for consideration of the specificities of local markets. To be considered representative, services should be subject to a fee at a minimum of one payment service provider in a Member State. In addition, where the services are common to a majority of Member States, the terminology used to define such services should be standardised at Union level, thus allowing for better comparison of payment account offers across the Union. In order to ensure sufficient homogeneity of the national lists, the European Supervisory Authority (European Banking Authority) (‘EBA’) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council (7) should issue guidelines to assist Member States to determine the services which are most commonly used and which generate the highest cost to consumers at national level. To that end, Member States should by 18 December 2014 indicate to the Commission and EBA the appropriate authorities to which those guidelines should be addressed.

(18) Once Member States have determined a provisional list of the most representative services subject to a fee at national level together with terms and definitions, EBA should review them to identify, the most of draft regulatory technical standards, the services that are common to the majority of Member States and propose standardised Union-level terms and definitions for them in all the official languages of the institutions of the Union. EBA should ensure that only one term is used for each service in any official language of each Member State which is also an official language of the institutions of the Union. This means that different terms can be used for the same service in different Member States sharing the same official language of the institutions of the Union, thereby taking into account national specificities. Member States should then integrate any applicable Union-level terms into their provisional lists and publish their final lists based on this.

(19) In order to help consumers compare payment account fees throughout the internal market easily, payment service providers should provide consumers with a fee information document that states the fees for all services contained in the list of the most representative services linked to a payment account at national level. The fee information document should where applicable use the standardised terms and definitions established at Union level. This would also contribute to establishing a level playing field between payment service providers competing in the payment account market. The fee information document should not contain any other fees. Where a payment service provider does not offer a service appearing in the list of the most representative services linked to a payment account, it should indicate this by, for example, marking the service as ‘not offered’ or ‘not applicable’. Member States should be able to require key indicators such as a comprehensive cost indicator summarising the overall annual cost of the payment account for consumers to be provided with the fee information document. In order to help consumers understand the fees they have to pay for their payment account, a glossary providing clear, non-technical and unambiguous explanations for at least the fees and services contained in the fee information document should be made available to them. The glossary should serve as a useful tool to encourage a better understanding of the meaning of fees, contributing towards empowering consumers to choose from a wider choice of payment account offers. An obligation should also be introduced requiring payment service providers to inform consumers, fee of charge and at least annually, of all the fees charged on their payment account including, if applicable, the overdraft interest rate, the credit interest rate. This is without prejudice to the provisions on overdrafts set out in Directive 2008/48/EC of the European Parliament and the Council (8). Ex post information should be provided in a dedicated document called a ‘statement of fees’. It should provide an overview of interest earned and all the fees incurred in relation to the use of the payment account to enable a consumer to understand what fee expenditures relate to and to assess the need to either modify consumption patterns or move to another provider. That benefit would be maximised by the ex post fee information presenting the most representative services in the same order as the ex ante fee information.

(21) In order to ensure consistent use of applicable Union-level terminology across the Union, Member States should establish an obligation requiring payment service providers to use the applicable Union-level terminology together with the remaining national standardised terminology identified in the final list when communicating with consumers, including in the fee information document and the statement of fees. Payment service providers should be able to use brand names in their contractual, commercial and marketing information to consumers, as long as they clearly identify the applicable
corresponding standardised term. Where they choose to use brand names in the fee information document or statement of fees, this should be in addition to the standardised terms as a secondary designation, such as in brackets or in a smaller font size.

(22) Comparison websites that are independent are an effective means for consumers to assess the merits of different payment account offers in one place. Such websites can provide right balance between the need for information to be clear and concise and the need for it to be complete and comprehensive, by enabling users to obtain more detailed information where this is of interest to them. They should aim at including the broadest possible range of offers, so as to give a representative overview, while also covering a significant part of the market. They can also reduce search costs as consumers will not need to collect information separately from payment service providers. It is crucial that the information given on such websites be trustworthy, impartial and transparent and that consumers be informed of the availability of such websites. In this regard, Member States should inform the public of such websites.

(23) In order to obtain impartial information on fees charged and interest rates applied in relation to payment accounts, consumers should be able to use publicly accessible comparison websites that are operationally independent from payment service providers, which means that no payment service provider should be given favourable treatment in search results. Member States should therefore ensure that consumers have free access to at least one such website in their respective territories. Such comparison websites may be operated by, or on behalf of, the competent authorities, other public authorities and/or private operators. The function of comparing fees connected to payment accounts may also be fulfilled by existing websites comparing a broad range of financial or non-financial products. Such websites should be operated in accordance with specified quality criteria including the requirement to provide details of their owners, to provide accurate and up-to-date information, to state the time of the last update, to set out clear, objective criteria on which the comparison will be based and to include a broad range of payment account offers covering a significant part of the market. Member States should be able to determine how often comparison websites are to review and update the information they provide to consumers, taking into account the frequency with which payment service providers generally update their fee information. Member States should also determine what constitutes a broad range of payment account offers covering a significant part of the market, by assessing, for example, how many payment service providers exist and therefore whether a simple majority or less would be sufficient and/or market share and/or their geographic location. A comparison website should compare the fees payable for services contained in the list of most representative services linked to payment accounts, integrating Union-level terminology. It is appropriate that Member States should be able to require such websites to compare other information, for example information on determinants of the level of services provided by payment service providers, such as the number and location of branches or automated teller machines. Where there is only one website in a Member State and that website ceases to operate or ceases to comply with the quality criteria, the Member State should ensure that consumers have access within a reasonable time to another comparison website at national level.

[...

(25) The process for switching payment accounts should be harmonised across the Union. At present, existing measures at national level are extremely diverse and do not guarantee an adequate level of consumer protection in all Member States. The provision of legislative measures establishing the main principles to be followed by payment service providers when providing such a service in each Member State would improve the functioning of the internal market for both consumers and payment service providers. On the one hand, it would guarantee a level playing field for consumers who may be interested in opening a payment account in a different Member State, as it would ensure that an equivalent level of protection is offered. On the other hand, it would reduce the differences between the regulatory measures in place at national level and would therefore reduce the administrative burden for payment service providers which intend to offer their services on a cross-border basis. As a consequence, the measures on switching would facilitate the provision of services related to payment accounts within the internal market.

(26) Switching should not imply the transfer of the contract from the transferring payment service provider to the receiving payment service provider.

(27) Consumers only have an incentive to switch payment accounts if the process does not entail an excessive administrative and financial burden. Therefore, payment service providers should offer to consumers a clear, quick and safe procedure to switch payment accounts, including payment accounts with basic features. Such a procedure should be guaranteed when consumers want to switch from one payment service provider to another, and also when consumers want to switch between different payment accounts within the same payment service provider. This would allow consumers to benefit from the most convenient offers on the market and to easily change from their existing payment account to potentially more suitable ones, irrespective of whether this occurs within the same payment service provider or between different payment service providers. Any fees charged by payment service providers in relation to the switching service should be reasonable and in line with the actual cost incurred by payment service providers.

(28) Member States should be allowed, with regard to switching where both payment service providers are located in their territory, to establish or maintain arrangements that differ from those provided for in this Directive if this is clearly in the interests of the consumer.

(29) The switching process should be as straightforward as possible for the consumer. Accordingly, Member States should ensure that the receiving payment service provider is responsible for initiating and managing the process on behalf of the consumer. Member States should be able to use additional means, such as technical solutions, when establishing the switching service. Such additional means may exceed the requirements of this Directive; for example, the switching service may be provided in a shorter time-frame or payment service providers may be required to ensure, upon a consumer’s request, the automated or manual routing of credit transfers received on the former payment account to the new payment account for a set limited period starting from receipt of the authorisation to switch. Such additional means may also be used by payment service providers on a voluntary basis even where this is not required by a Member State.

(30) Consumers should be allowed to ask the receiving payment service provider to switch all or part of the incoming credit transfers, standing orders for credit transfers or direct debit mandates, ideally within a single meeting with the receiving payment service provider. To that end, consumers should be able to sign one authorisation giving consent to each of the above movements to take place. Member States could require that the authorisation from the consumer be in writing, but could also choose to accept equivalent means where appropriate, for example where an automated system for switching is in place. Before giving the authorisation, the consumer should be informed of all the steps of the procedure necessary to complete the switching. For example, the authorisation could include all the tasks that form part of the switching service and could allow for the possibility of the consumer choosing only some of those tasks.

[...

(32) In order to facilitate cross-border account-opening, the consumer should be allowed to ask the new payment service
provider to set up on the new payment account all or part of standing orders for credit transfers, accept direct debits from the date specified by the consumer, and provide the consumer with information giving details of the new payment account, preferably within a single meeting with the new payment service provider.

(33) Consumers should not be subject to financial losses, including charges and interest, caused by any mistakes made by either of the payment service providers involved in the switching process. In particular, consumers should not bear any financial loss deriving from the payment of additional fees, interest or other charges as well as fines, penalties or any other type of financial detriment due to delay in the execution of the payment.

(34) Member States should guarantee that consumers who intend to open a payment account are not discriminated against on the basis of their nationality or place of residence. While it is important for credit institutions to ensure that their customers are not using the financial system for illegal purposes such as fraud, money laundering or terrorism financing, they should not impose barriers to consumers who want to benefit from the advantages of the internal market by opening and using payment accounts on a cross-border basis. Therefore, the provisions of Directive 2005/60/EC of the European Parliament and of the Council (9) should not be used as a pretext for rejecting commercially less attractive consumers.

(37) Member States should be able, in full respect of the fundamental freedoms guaranteed by the Treaties, to require consumers who wish to open a payment account with basic features in their territory to show a genuine interest in doing so. Without prejudice to the requirements adopted in conformity with Directive 2005/60/EC to prevent money laundering, physical attendance at the premises of the credit institutions should not be required in order to show such a genuine interest.

(45) In the process of identifying the services to be offered with a payment account with basic features and the minimum number of operations to be included, national specificities should be taken into account. In particular, certain services may be considered essential in guaranteeing full use of a payment account in a certain Member State, due to their widespread use at the national level. For example, in some Member States consumers still widely use cheques, while that means of payment is very rarely used in other Member States. This Directive should therefore allow Member States to identify additional services that are considered essential at national level and which should be provided with a payment account with basic features. For example, Member States should consider the use of specific services targeted and, in particular, that they reach out to unbanked, vulnerable and mobile consumers. Credit institutions should actively make available to consumers accessible information and adequate assistance about the specific features of the payment account with basic features on offer, their associated fees and their conditions of use, and also the steps consumers should take to exercise their right to open a payment account with basic features. In particular, consumers should be informed that the purchase of additional services is not compulsory in order to access a payment account with basic features.

(46) In order to ensure that payment accounts with basic features are available to the widest possible range of consumers, they should be offered free of charge or for a reasonable fee. To encourage unbanked vulnerable consumers to participate in the retail banking market, Member States should be able to provide that payment accounts with basic features are to be offered to those consumers on particularly advantageous terms, such as free of charge. Member States should be free to define the mechanism to identify those consumers that can benefit from payment accounts with basic features on more advantageous terms, provided that the mechanism ensures that vulnerable consumers can access a payment account with basic features. In any event, such an approach should be without prejudice to the right of all consumers, including non-vulnerable ones, to access payment accounts with basic features at least at a reasonable fee. Furthermore, any additional charges to the consumer for non-compliance with the terms laid down in the contract should be reasonable. Member States should establish what constitutes a reasonable charge according to national circumstances.

(47) Credit institutions should refuse to open or should terminate a contract for a payment account with basic features only in specific circumstances, such as non-compliance with the legislation on money laundering and terrorist financing or on the prevention and investigation of crimes. Even in those cases, a refusal can only be justified where the consumer does not comply with that legislation and not because the procedure to check compliance with the legislation is too burdensome or costly. In any event, Member States should be able to permit credit institutions to take measures against consumers who have committed a crime, such as a serious fraud against a credit institution, with a view to avoiding a recurrence of such a crime. Such measures should include, for example, limiting access by that consumer to a payment account with basic features for a certain period of time. Besides, there may be cases in which the previous refusal of an application for a payment account may be necessary in order to identify consumers who could benefit from a payment account on more advantageous terms. In such a case, the credit institution should inform the consumer that he may use a specific mechanism in the event of refusal of an application for a payment account for which a fee is charged as provided for in this Directive to obtain access to a payment account with basic features that is free of charge. Both such additional cases should, however, be limited, specific and based on precisely identified provisions of national law. When identifying additional cases in which credit institutions can refuse to offer payment accounts to consumers, Member States should be able to include, inter alia, grounds of public security or public policy.

(48) Clear and comprehensible information on the right to open and use a payment account with basic features should be provided by Member States and credit institutions to consumers. Member States should ensure that communication measures are well-targeted and, in particular, that they reach out to unbanked, vulnerable and mobile consumers. Credit institutions should actively make available to consumers accessible information and adequate assistance about the specific features of the payment account with basic features on offer, their associated fees and their conditions of use, and also the steps consumers should take to exercise their right to open a payment account with basic features. In particular, consumers should be informed that the purchase of additional services is not compulsory in order to access a payment account with basic features.
HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter and scope

1. This Directive lays down rules concerning the transparency and comparability of fees charged to consumers on their payment accounts held within the Union, rules concerning the switching of payment accounts within a Member State and rules to facilitate cross-border payment account-opening for consumers.

2. This Directive also defines a framework for the rules and conditions according to which Member States are required to guarantee a right for consumers to open and use payment accounts with basic features in the Union.

3. Chapters II and III apply to payment service providers.

4. Chapter IV applies to credit institutions.

Member States may decide to apply Chapter IV to payment service providers other than credit institutions.

5. Member States may decide not to apply all or part of this Directive to the entities referred to in Article 2(5) of Directive 2013/36/EU of the European Parliament and of the Council (17).

6. This Directive applies to payment accounts through which consumers are able at least to:

(a) place funds in a payment account;
(b) withdraw cash from a payment account;
(c) execute and receive payment transactions, including credit transfers, to and from a third party.

Member States may decide to apply all or part of this Directive to payment accounts other than those referred to in the first subparagraph.

7. The opening and use of a payment account with basic features pursuant to this Directive shall be in conformity with Directive 2005/60/EC.

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'consumer' means any natural person who is acting for purposes which are outside his trade, business, craft or profession;

(2) 'legally resident in the Union' means where a natural person has the right to reside in a Member State by virtue of Union or national law, including consumers with no fixed address and persons seeking asylum under the Geneva Convention of 28 July 1951 Relating to the Status of Refugees, the Protocol thereto of 31 January 1967 and other relevant international treaties;

(3) 'payment account' means an account held in the name of one or more consumers which is used for the execution of payment transactions;

(4) 'payment service' means a payment service as defined in point (3) of Article 4 of Directive 2007/64/EC;

(5) 'payment transaction' means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

(6) 'services linked to the payment account' means all services related to the opening, operating and closing of a payment account, including payment services and payment transactions falling within the scope of point (g) of Article 3 of Directive 2007/64/EC and overdraft facilities and overrunning;

(7) 'payment service provider' means a payment service provider as defined in point (9) of Article 4 of Directive 2007/64/EC;

(8) 'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (18);

(9) 'payment instrument' means a payment instrument as defined in point (23) of Article 4 of Directive 2007/64/EC;

(10) 'transferring payment service provider' means the payment service provider from which the information required to perform the switching is transferred;

(11) 'receiving payment service provider' means the payment service provider to which the information required to perform the switching is transferred;

(12) 'payment order' means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;

(13) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payer's payment account, a natural or legal person who makes a payment order to a payee's payment account;

(14) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

(15) 'fees' means all charges and penalties, if any, payable by the consumer to the payment service provider for or in relation to services linked to a payment account;

(16) 'credit interest rate' means any rate at which interest is paid to the consumer in respect of funds held in a payment account;

(17) 'durable medium' means any instrument which enables the consumer to store information addressed personally to that consumer in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(18) 'switching' or 'switching service' means, upon a consumer's request, transferring from one payment service provider to another either the information about all or some standing orders for credit transfers, recurring direct debits and recurring incoming credit transfers executed on a payment account, or any positive payment account balance from one payment account to the other, or both, with or without closing the former payment account;

(19) 'direct debit' means a national or cross-border payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent;

(20) 'credit transfer' means a national or cross-border payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer;

(21) 'standing order' means an instruction given by the payer to the payment service provider which holds the payer's payment account to execute credit transfers at regular intervals or on predetermined dates;

(22) 'funds' means banknotes and coins, scriptural money, and electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council (19);

(23) 'framework contract' means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;

(24) 'business day' means a day on which the relevant payment service provider is open for business as required for the execution of a payment transaction;

(25) 'overdraft facility' means an explicit credit agreement whereby a payment service provider makes available to a consumer funds which exceed the current balance in the consumer's payment account;

(26) 'overrunning' means a tacitly accepted overdraft whereby a payment service provider makes available to a consumer funds which exceed the current balance in the consumer's payment account or the agreed overdraft facility;

(27) 'competent authority' means an authority designated as competent by a Member State in accordance with Article 21.

CHAPTER II
COMPARABILITY OF FEES CONNECTED WITH PAYMENT ACCOUNTS

Article 3
List of the most representative services linked to a payment account and subject to a fee at national level and standardised terminology

1. Member States shall establish a provisional list of at least 10 and no more than 20 of the most representative services linked to a payment account and subject to a fee, offered by at least one payment service provider at national level. The list shall contain terms and definitions for each of the services identified. In any official language of a Member State, only one term shall be used for each service.

2. For the purposes of paragraph 1, the Member States shall have regard to the services that:
   (a) are most commonly used by consumers in relation to their payment account;
   (b) generate the highest cost for consumers, both overall as well as per unit.

In order to ensure the sound application of the criteria set out in the first subparagraph of this paragraph, EBA shall issue guidelines pursuant to Article 16 of Regulation (EU) No 1093/2010 by 18 March 2015.

3. Member States shall notify to the Commission and to EBA the provisional lists referred to in paragraph 1 by 18 September 2015. On request, Member States shall provide the Commission with supplementary information concerning the data on the basis of which they have compiled those lists with regard to the criteria set out in paragraph 2.

4. On the basis of the provisional lists notified pursuant to paragraph 3, EBA shall develop draft regulatory technical standards setting out the Union standardised terminology for those services that are common to at least a majority of Member States. The Union standardised terminology shall include common terms and definitions for the common services and shall be made available in the official languages of the institutions of the Union. In any official language of a Member State, only one term shall be used for each service.

EBA shall submit those draft regulatory technical standards to the Commission by 18 September 2016.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010.

5. Member States shall integrate the Union standardised terminology established under paragraph 4 into the provisional list referred to in paragraph 1 and shall publish the resulting final list of the most representative services linked to a payment account without delay and at the latest within three months after the delegated act referred to in paragraph 4 has entered into force.

6. Every four years, following publication of the final list referred to in paragraph 5, Member States shall assess and, where appropriate, update the list of the most representative services established pursuant to paragraphs 1 and 2. They shall notify to the Commission and to EBA the outcome of their assessment and, where applicable, of the updated list of the most representative services. EBA shall review and, where necessary, update the Union standardised terminology in accordance with the process set out in paragraph 4. Upon the Union standardised terminology being updated, Member States shall update and publish their final list as referred to in paragraph 5 and shall ensure that payment service providers use the updated terms and definitions.

Article 4
Fee information document and glossary

1. Without prejudice to Article 42(3) of Directive 2007/64/EC and Chapter II of Directive 2008/48/EC, Member States shall ensure that, in good time before entering into a contract for a payment account with a consumer, payment service providers provide the consumer with a fee information document on paper or another durable medium containing the standardised terms in the final list of the most representative services linked to a payment account referred to in Article 3(5) of this Directive and, where such services are offered by a payment service provider, the corresponding fees for each service.

2. The fee information document shall:
   (a) be a short and stand-alone document;
   (b) be presented and laid out in a way that is clear and easy to read, using characters of a readable size;
   (c) be no less comprehensible in the event that, having been originally produced in colour, it is printed or photocopied in black and white;
   (d) be written in the official language of the Member State where the payment account is offered or, if agreed by the consumer and the payment service provider, in another language;
   (e) be accurate, not misleading and expressed in the currency of the payment account or, if agreed by the consumer and the payment service provider, in another currency of the Union;
   (f) contain the title ‘fee information document’ at the top of the first page next to a common symbol to distinguish the document from other documentation; and
   (g) include a statement that it contains fees for the most representative services related to the payment account and that complete pre-contractual and contractual information on all the services is provided in other documents.

Member States may determine that, for the purposes of paragraph 1, the fee information document shall be provided together with information required pursuant to other Union or national legislative acts on payment accounts and related services on the condition that all the requirements of the first subparagraph of this paragraph are met.

3. Where one or more services are offered as part of a package of services linked to a payment account, the fee information document shall disclose the fee for the entire package, the services included in the package and their quantity, and the additional fee for any service that exceeds the quantity covered by the package fee.

4. Member States shall establish an obligation for payment service providers to make available to consumers a glossary of at least the standardised terms set out in the final list referred to in Article 3(5) and the related definitions.

Power is conferred on the Commission to adopt the regulatory technical standards referred to in the first subparagraph, including other definitions, if any, is drafted in clear, unambiguous and non-technical language and that it is not misleading.

5. The fee information document and the glossary shall be made available to consumers at any time by payment service providers. They shall be provided in an easily accessible manner, including to non-customers, in electronic form on their websites where available and in the premises of payment service providers accessible to consumers. They shall also be provided on paper or another durable medium free of charge upon request by a consumer.

6. EBA, after consulting national authorities and after consumer testing, shall develop draft implementing technical standards regarding a standardised presentation format of the fee information document and its common symbol. EBA shall submit those draft implementing technical standards to the Commission by 18 September 2016.

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph of this paragraph in accordance with Article 15 of Regulation (EU) No 1093/2010.

7. Following the updating of the Union standardised terminology pursuant to Article 3(6), EBA shall, where necessary, review and update the standardised presentation format of the fee information document and its common symbol, following the procedure set out in paragraph 6 of this Article.

Article 5
Statement of fees
1. Without prejudice to Articles 47 and 48 of Directive 2007/64/EC and Article 12 of Directive 2008/48/EC, Member States shall ensure that payment service providers provide the consumer, at least annually and free of charge, with a statement of all fees incurred, as well as, where applicable, information regarding the interest rates referred to in points (c) and (d) of paragraph 2 of this Article, for services linked to a payment account. Where applicable, payment service providers shall use the standardised terms set out in the final list referred to in Article 3(5) of this Directive. The communication channel used to provide the statement of fees shall be agreed with the consumer. The statement of fees shall be provided on paper at least upon the request of the consumer.

2. The statement of fees shall specify at least the following information:
   (a) the unit fee charged for each service and the number of times the service was used during the relevant period, and where the services are combined in a package, the fee charged for the package as a whole, the number of times the package fee was charged during the relevant period and the additional fee charged for any service exceeding the quantity covered by the package fee;
   (b) the total amount of fees incurred during the relevant period for each service, each package of services provided and services exceeding the quantity covered by the package fee;
   (c) the overdraft interest rate applied to the payment account and the total amount of interest charged relating to the overdraft during the relevant period, where applicable;
   (d) the credit interest rate applied to the payment account and the total amount of interest earned during the relevant period, where applicable;
   (e) the total amount of fees charged for all services provided during the relevant period.

3. The statement of fees shall:
   (a) be presented and laid out in a way that is clear and easy to read, using characters of a readable size;
   (b) be accurate, not misleading and expressed in the currency of the payment account or, if agreed by the consumer and the payment service provider, in another currency;
   (c) contain the title ‘statement of fees’ at the top of the first page of the statement next to a common symbol to distinguish the document from other documentation; and
   (d) be written in the official language of the Member State where the payment account is offered or, if agreed by the consumer and the payment service provider, in another language.

Member States may determine that the statement of fees shall be provided together with information required pursuant to other Union or national legislative acts on payment accounts and related services as long as all the requirements of the first subparagraph are met.

4. EBA, after consulting national authorities and after consumer testing, shall develop implementing technical standards regarding a standardised presentation format of the statement of fees and its common symbol. EBA shall submit the draft implementing technical standards referred to in the first subparagraph to the Commission by 18 September 2016.

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph of this paragraph in accordance with Article 15 of Regulation (EU) No 1093/2010.

5. Following the updating of the Union standardised terminology pursuant to Article 3(6), EBA shall, where necessary, review and update the standardised presentation format of the statement of fees and its common symbol, following the procedure set out in paragraph 4 of this Article.

Article 6

Information for consumers

1. Member States shall ensure that in their contractual, commercial and marketing information to consumers, payment service providers use, where applicable, the standardised terms set out in the final list referred to in Article 3(5). Payment service providers may use brand names in the fee information document and in the statement of fees, provided such brand names are used in addition to the standardised terms set out in the final list referred to in Article 3(5) as a secondary designation of those services.

2. Payment service providers may use brand names to designate their services in their contractual, commercial and marketing information to consumers, provided that they clearly identify, where applicable, the corresponding standardised terms set out in the final list referred to in Article 3(5).

Article 7

Comparison websites

1. Member States shall ensure that consumers have access, free of charge, to at least one website comparing fees charged by payment service providers for at least the services included in the final list referred to in Article 3(5) at national level. Comparison websites may be operated either by a private operator or by a public authority.

2. Member States may require the comparison websites referred to in paragraph 1 to include further comparative determinants relating to the level of service offered by the payment service provider.

3. The comparison websites established in accordance with paragraph 1 shall:
   (a) be operationally independent by ensuring that payment service providers are given equal treatment in search results;
   (b) clearly disclose their owners;
   (c) set out clear, objective criteria on which the comparison will be based;
   (d) use plain and unambiguous language and, where applicable, the standardised terms set out in the final list referred to in Article 3(5);
   (e) provide accurate and up-to-date information and state the time of the last update;
   (f) include a broad range of payment account offers covering a significant part of the market and, where the information presented is not a complete overview of the market, a clear statement to that effect, before displaying results; and
   (g) provide an effective procedure to report incorrect information on published fees.

4. Member States shall ensure that information is made available online about the availability of websites that comply with this Article.

Article 8

Payment accounts packaged with another product or service

Member States shall ensure that, when a payment account is offered as part of a package together with another product or service which is not linked to a payment account, the payment service provider informs the consumer whether it is possible to purchase the payment account separately and, if so, provides separate information regarding the costs and fees associated with each of the other products and services offered in that package that can be purchased separately.

CHAPTER III

SWITCHING

Article 9

Provision of the switching service

Member States shall ensure that payment service providers provide a switching service as described in Article 10 between payment accounts held in the same currency to any consumer who opens or holds a payment account with a payment service provider located in the territory of the Member State concerned.

Article 10

The switching service

1. Member States shall ensure that the switching service is initiated by the receiving payment service provider at the
request of the consumer. The switching service shall at least comply with paragraphs 2 to 6.

Member States may establish or maintain measures alternative to those referred to in paragraphs 2 to 6, provided that:

(a) it is clearly in the interest of the consumer;
(b) there is no additional burden for the consumer; and
(c) the switching is completed within, as a maximum, the same overall time-frame as that indicated in paragraphs 2 to 6.

2. The receiving payment service provider shall perform the switching service upon receipt of the authorisation from the consumer. In the case of two or more holders of the account, authorisation shall be obtained from each of them.

The authorisation shall be drawn up in an official language of the Member State where the switching service is being initiated or in any other language agreed between the parties. The authorisation shall allow the consumer to provide specific consent to the performance by the transferring payment service provider of each of the tasks referred to in paragraph 3 and to provide specific consent to the performance by the receiving payment service provider of each of the tasks referred to in paragraph 5.

The authorisation shall allow the consumer to specifically identify incoming credit transfers, standing orders for credit transfers and direct debit mandates that are to be switched. The authorisation shall also allow consumers to specify the date from which standing orders for credit transfers and direct debits are to be executed from the payment account opened or held with the receiving payment service provider. That date shall be at least six business days after the date on which the receiving payment service provider receives the documents transferred from the transferring payment service provider pursuant to paragraph 4. Member States may require the authorisation from the consumer to be in writing and that a copy of the authorisation be provided to the consumer.

3. Within two business days from receipt of the authorisation referred to in paragraph 2, the receiving payment service provider shall request the transferring payment service provider to carry out the following tasks, if provided for in the consumer’s authorisation:

(a) transmit to the receiving payment service provider and, if specifically requested by the consumer, to the consumer, a list of the existing standing orders for credit transfers and available information on direct debit mandates that are being switched;

(b) transmit to the receiving payment service provider and, if specifically requested by the consumer, to the consumer, the available information about recurring incoming credit transfers and creditor-driven direct debits executed on the consumer’s payment account in the previous 13 months;

(c) where the transferring payment service provider does not provide a system for automated redirection of the incoming credit transfers and direct debits to the payment account held by the consumer with the receiving payment service provider, stop accepting direct debits and incoming credit transfers with effect from the date specified in the authorisation;

(d) transfer any remaining positive balance from the payment account opened or held by the consumer with the receiving payment service provider to the payer or the payee of the reason for not accepting the payment transaction;

(e) without prejudice to Article 45(1) and (6) of Directive 2007/64/EC, close the payment account on the date specified in the authorisation if the consumer has no outstanding obligations on that payment account or the consumer enables the actions listed in points (a), (b) and (d) of this paragraph have been completed. The payment service provider shall immediately inform the consumer where such outstanding obligations prevent the consumer’s payment account from being closed.

5. Within five business days of receipt of the information requested from the transferring payment service provider as referred to in paragraph 3, the receiving payment service provider shall, as and if provided for in the authorisation and to the extent that the information provided by the transferring payment service provider or the consumer enables the receiving payment service provider to do so, carry out the following tasks:

(a) set up the standing orders for credit transfers requested by the consumer and execute them with effect from the date specified in the authorisation;

(b) make any necessary preparations to accept direct debits and accept them with effect from the date specified in the authorisation;

(c) where relevant, inform consumers of their rights pursuant to point (d) of Article 5(3) of Regulation (EU) No 260/2012;

(d) inform payers specified in the authorisation and making recurring incoming credit transfers into a consumer’s payment account of the details of the consumer’s payment account with the receiving payment service provider and transmit to the payers a copy of the consumer’s authorisation. If the receiving payment service provider does not have all the information it needs to inform the payers, it shall ask the consumer or the transferring payment service provider to provide the missing information;

(e) inform payees specified in the authorisation and using a direct debit to collect funds from the consumer’s payment account of the details of the consumer’s payment account with the receiving payment service provider and transmit to the payees a copy of the consumer’s authorisation. If the receiving payment service provider does not have all the information it needs to inform the payees, it shall ask the consumer or the transferring payment service provider to provide the missing information.

Where the consumer chooses to personally provide the information referred to in points (d) and (e) of the first subparagraph of this paragraph to the payers or payees rather than provide specific consent in accordance with paragraph 2 to the receiving payment service provider to do so, the receiving payment service provider shall provide the consumer with standard letters providing details of the payment account and the starting date specified in the authorisation within the deadline referred to in the first subparagraph of this paragraph.

6. Without prejudice to Article 55(2) of Directive 2007/64/EC, the transferring payment service provider shall not block payment instruments before the date specified in the consumer’s authorisation, so that the provision of payment services to the consumer is not interrupted in the course of the provision of the switching service.
Article 11
Facilitation of cross-border account-opening for consumers
1. Member States shall ensure that where a consumer indicates to his payment service provider that he wishes to open a payment account with a payment service provider located in another Member State, the payment service provider with which the consumer holds a payment account shall on receipt of such request provide the following assistance to the consumer:
(a) provide the consumer free of charge with a list of all the currently active standing orders, the person or creditor-driven direct debit mandates, where available, and with available information about recurring incoming credit transfers and debtor-driven direct debits executed on the consumer’s payment account in the previous 13 months. That list shall not entail any obligation on the part of the new payment service provider to set up services that it does not provide;
(b) transfer any positive balance remaining on the payment account held by the consumer to the payment account opened or held by the consumer with the new payment service provider, provided that the request includes full details allowing the new payment service provider and the consumer’s payment account to be identified;
(c) close the payment account held by the consumer.
2. Without prejudice to Articles 45(1) and 45(6) of Directive 2007/64/EC and if the consumer has no outstanding obligations with the payment service provider with which the consumer holds that payment account shall conclude the steps set out in points (a), (b) and (c) of paragraph 1 of this Article on the date specified by the consumer, which shall be at least six business days after that payment service provider receives the consumer’s request unless otherwise agreed between the parties. The payment service provider shall immediately inform the consumer where outstanding obligations prevent his payment account from being closed.

Article 12
Fees connected with the switching service
1. Member States shall ensure that consumers are able to access free of charge their personal information regarding existing standing orders and direct debits held by either the transferring or the receiving payment service provider.
2. Member States shall ensure that the transferring payment service provider provides the information referred to in paragraph 1 to the receiving payment service provider pursuant to point (a) of Article 10(4) without charging the consumer or the receiving payment service provider.
3. Member States shall ensure that fees, if any, applied by the transferring or the receiving payment service provider to the consumer for any service provided under Article 10, other than those referred to in paragraphs 1, 2 and 3 of this Article, are reasonable and in line with the actual costs of that payment service provider.

Article 13
Financial loss for consumers
1. Member States shall ensure that any financial loss, including charges and interest, incurred by the consumer and resulting directly from the non-compliance of a payment service provider involved in the switching process with its obligations under Article 10 is refunded by that payment service provider without delay.
2. Liability under paragraph 1 shall not apply in cases of abnormal and unforeseeable circumstances beyond the control of the payment service provider pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by Union or national legislative acts.
3. Member States shall ensure that liability under paragraphs 1 and 2 is established in accordance with the legal requirements applicable at national level.

Article 14
Information about the switching service
1. Member States shall ensure that payment service providers make available to consumers the following information about the switching service:
(a) the roles of the transferring and receiving payment service provider for each step of the switching process, as indicated in Article 10;
(b) the time-frame for completion of the respective steps;
(c) the fees, if any, charged for the switching process;
(d) any information that the consumer will be asked to provide;
(e) the alternative dispute resolution procedures referred to in Article 24.
2. Member States may require that payment service providers also make available other information, including, where applicable, the information necessary for the identification of the deposit guarantee scheme within the Union of which the payment service provider is a member.

CHAPTER IV
ACCESS TO PAYMENT ACCOUNTS

Article 15
Non-discrimination
Member States shall ensure that credit institutions do not discriminate against consumers legally resident in the Union by reason of their nationality or place of residence or by reason of any other ground as referred to in Article 21 of the Charter, when those consumers apply for or access a payment account within the Union. The conditions applicable to holding a payment account with basic features shall be in no way discriminatory.

Article 16
Right of access to a payment account with basic features
1. Member States shall ensure that payment accounts with basic features are offered to consumers by all credit institutions or a sufficient number of credit institutions to guarantee access thereto for all consumers in their territory, and to prevent distortions of competition. Member States shall ensure that payment accounts with basic features are not only offered by credit institutions that provide payment accounts with solely online facilities.
2. Member States shall ensure that consumers legally resident in the Union, including consumers with no fixed address and asylum seekers, and consumers who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons, have the right to open and use a payment account with basic features located in their territory. Such a right shall apply irrespective of the consumer’s place of residence.

Member States may, in full respect of the fundamental freedoms guaranteed by the Treaties, require consumers who wish to open a payment account with basic features in their territory to show a genuine interest in doing so.

Member States shall ensure that the exercise of the right is not made too difficult or burdensome for the consumer.
3. Member States shall ensure that credit institutions offering payment accounts with basic features open the payment account with basic features or refuse a consumer’s application for a payment account with basic features, in each case
without undue delay and at the latest 10 business days after receiving a complete application.  
4. Member States shall ensure that credit institutions refuse an application for a payment account with basic features where opening such an account would result in an infringement of the provisions on the prevention of money laundering and the countering of terrorist financing laid down in Directive 2005/60/EC.

5. Member States may permit credit institutions that offer payment accounts with basic features to refuse an application for such an account where a consumer already holds a payment account with a credit institution located in their territory which allows him to make use of the services listed in Article 17(1), save where a consumer declares that he has received notice that a payment account will be closed. In such cases, before opening a payment account with basic features, the credit institution may verify whether the consumer holds or does not hold a payment account with a credit institution located in the same Member State which enables consumers to make use of the services listed in Article 17(1). Credit institutions may rely on a declaration of honour signed by consumers for that purpose.

6. Member States may identify limited and specific additional cases where credit institutions may be required or may choose to refuse an application for a payment account with basic features. Such cases shall be based on provisions of national law applicable in their territory and shall be aimed either at facilitating access by the consumer to a payment account with basic features free of charge under the mechanism of Article 25 or at avoiding abuses by consumers of their right to access a payment account with basic features.

7. Member States shall ensure that, in the cases referred to in paragraphs 4, 5 and 6, after taking its decision, the credit institution immediately informs the consumer of the refusal and of the specific reason for that refusal, in writing and free of charge, unless such disclosure would be contrary to objectives of national security, public policy or Directive 2005/60/EC. In the event of refusal, the credit institution shall advise the consumer of the procedure to submit a complaint and of the specific reason for that refusal, in writing and free of charge.

8. Member States shall ensure that a payment account with basic features allows consumers to execute an unlimited number of operations in relation to the services referred to in paragraph 1.

9. With respect to the services referred to in points (a), (b), (c) and (d)(ii) of paragraph 1 of this Article excluding payment transactions through a credit card, Member States shall ensure that credit institutions do not charge any fees beyond the reasonable fees, if any, referred to in Article 18, irrespective of the number of operations executed on the payment account.

10. With respect to payments referred to in point (d)(i) of paragraph 1 of this Article, point (d)(ii) of paragraph 1 of this Article only as regards payment transactions through a credit card and point (d)(iii) of paragraph 1 of this Article, Member States may determine a minimum number of operations for which credit institutions can only charge the reasonable fees, if any, referred to in Article 18. Member States shall ensure that the minimum number of operations is sufficient to cover the personal use by the consumer, taking into account existing consumer behaviour and common commercial practices. The fees charged for operations above the minimum number of operations shall never be higher than those charged under the usual pricing policy of the credit institution.

11. Member States shall ensure that the consumer is able to manage and initiate payment transactions from the consumer’s payment account with basic features in the credit institution’s premises and/or via online facilities, where available.

12. Without prejudice to the requirements laid down in Directive 2008/48/EC, Member States may allow credit institutions to provide, upon the consumer’s request, an overdraft facility in relation to a payment account with basic features. Member States may define a maximum amount and a maximum duration of any such overdraft. Access to, or use of, the payment account with basic features shall not be restricted by, or made conditional on, the purchase of such credit services.

Article 18

Associated fees
1. Member States shall ensure that the services referred to in Article 17 are offered by credit institutions free of charge or for a reasonable fee.

2. Member States shall ensure that the fees charged to the consumer for non-compliance with the consumer’s commitments laid down in the framework contract are reasonable.

3. Member States shall ensure that the reasonable fees referred to in paragraphs 1 and 2 are established taking into account at least the following criteria: (a) national income levels; (b) average fees charged by credit institutions in the Member State concerned for services provided on payment accounts.

4. Without prejudice to the right referred to in Article 16(2) and the obligation contained in paragraph 1 of this Article, Member States may require credit institutions to implement various pricing schemes depending on the level of banking

Institute of Law and Technology
Masaryk University, Faculty of Law
inclusion of the consumer, allowing for, in particular, more advantageous conditions for unbanked vulnerable consumers. In such cases, Member States shall ensure that consumers are provided with guidance, as well as adequate information, on the available options.

[...] CHAPTER V
COMPETENT AUTHORITIES AND ALTERNATIVE DISPUTE RESOLUTION

Article 21
Competent authorities
1. Member States shall designate the national competent authorities empowered to ensure the application and enforcement of this Directive and shall ensure that they are granted investigation and enforcement powers and adequate resources necessary for the efficient and effective performance of their duties.

The competent authorities shall be either public authorities or bodies recognised by national law or by public authorities expressly empowered for that purpose by national law. They shall not be payment service providers, with the exception of national central banks.

2. Member States shall ensure that competent authorities and all persons who work or who have worked for competent authorities, as well as auditors and experts instructed by competent authorities, are bound by the obligation of professional secrecy. No confidential information which they may receive in the course of their duties may be divulged to any person or authority whatsoever, save in summary or aggregate form, without prejudice to cases covered by criminal law or by this Directive. This shall not, however, prevent competent authorities from exchanging or transmitting confidential information in accordance with Union and national law.

3. Member States shall ensure that the authorities designated as competent for ensuring the application and enforcement of this Directive are either or both of the following:
   (a) competent authorities as defined in point (2) of Article 4 of Regulation (EU) No 1093/2010;
   (b) authorities other than the competent authorities referred to in point (a) that provided that national laws, regulations or administrative provisions require those authorities to cooperate with the competent authorities referred to in point (a) whenever necessary in order to carry out their duties under this Directive, including for the purposes of cooperating with EBA as required under this Directive.

4. Member States shall notify the Commission and EBA of the competent authorities and of any changes thereto. The first such notification shall be made as soon as possible and at the latest by 18 September 2016.

5. The competent authorities shall exercise their powers in conformity with national law either:
   (a) directly under their own authority or under the supervision of the judicial authorities;
   (b) by application to courts which are competent to grant the necessary decision, including, where appropriate, by appeal, if the application to grant the necessary decision is not successful.

6. Where there is more than one competent authority on their territory, Member States shall ensure that their respective duties are clearly defined and that those authorities collaborate closely so that they can discharge their respective duties effectively.

7. The Commission shall publish a list of the competent authorities in the Official Journal of the European Union at least once a year, and update it continuously on its website.

[...] Article 25
Mechanism in the event of refusal of a payment account for which a fee is charged

Without prejudice to Article 16, Member States may set up a specific mechanism to ensure that consumers who do not have a payment account in their territory and who have been denied access to a payment account for which a fee is charged by credit institutions will have effective access to a payment account with basic features, free of charge.

[...] CHAPTER VII
FINAL PROVISIONS

[...] Article 29
Transposition

By 18 September 2016, Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately communicate to the Commission the text of those measures.

2. They shall apply the measures referred to in paragraph 1 from 18 September 2016.

By way of derogation from the first subparagraph:
   (a) Article 3 shall apply from 17 September 2014;
   (b) Member States shall apply the measures necessary to comply with Article 4(1) to (5), Article 5(1), (2) and (3), Article 6(1) and (2) and Article 7 by nine months after the entry into force of the delegated act referred to in Article 3(4);
   (c) Member States in which the equivalent of a fee information document at national level already exists may choose to integrate the common format and its common symbol at the latest 18 months after the entry into force of the delegated act referred to in Article 3(4);
   (d) Member States in which the equivalent of a statement of fees at national level already exists may choose to integrate the common format and its common symbol at the latest 18 months after the entry into force of the delegated act referred to in Article 3(4).

3. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

4. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

Article 30
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 31
Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels, 23 July 2014.

For the European Parliament
The President
M. SCHULZ

For the Council
The President
S. GOZI
Relevant EU Regulations and Directive on European Union Supervisory Bodies


Relevant Case Law on Distant Marketing in Investments

C-384/93 Alpine Investments v. Minister van Financiën (Minister for Finance)

1 By order of 28 April 1993, received at the Court on 6 August 1993, the College van Beroep voor het Bedrijfsleven (Administrative Court for Trade and Industry; hereinafter "the Administrative Court") referred to the Court for a preliminary ruling under Article 177 of the EEC Treaty several questions on the interpretation of Article 59 of the Treaty.

2 Those questions were raised in proceedings brought by Alpine Investments BV challenging the restriction imposed on it by the Netherlands Ministry of Finance prohibiting it from contacting individuals by telephone without their prior consent in writing in order to offer them various financial services (a practice known as "cold calling").

3 Alpine Investments BV, the applicant in the main proceedings (hereinafter "Alpine Investments"), is a company incorporated under Netherlands law and established in the Netherlands which specializes in commodities futures.

4 The parties to a commodities futures contract undertake to buy or sell a specified quantity of a commodity of a given quality at a price and date fixed at the time the contract is concluded. They do not, however, intend actually to take delivery of or to deliver the commodity but contract solely in the hope of profiting from price fluctuations between the time the contract is concluded and the month of delivery. This can be done by entering into a mirror-image transaction on the futures market before the beginning of the month of delivery.

5 Alpine Investments offers three types of service in relation to commodities futures contracts: portfolio management, investment advice and the transmission of clients’ orders to brokers operating on commodities futures markets both within and outside the Community. It has clients not only in the Netherlands but also in Belgium, France and the United Kingdom. It is not however established anywhere outside the Netherlands.

6 At the time of the events which gave rise to the main proceedings, financial services were governed in the Netherlands by the Wet Effectenhandel (Law on Securities Transactions) of 30 October 1985. Article 6(1) of that law prohibited a person from acting as an intermediary in securities transactions without a licence. Article 8(1) empowered the Minister for Finance to grant an exemption permitting it to place orders with a specified broker, Merrill Lynch Inc. The exemption required Alpine Investments to comply with any rules which might be issued by the Minister for Finance in the near future regarding its contacts with potential clients.

7 On 6 September 1991 the Minister for Finance, respondent in the main proceedings, granted Alpine Investments an exemption permitting it to place orders with a specified broker, Merrill Lynch Inc. The exemption required Alpine Investments to comply with any rules which might be issued by the Minister for Finance in the near future regarding its contacts with potential clients.

8 On 1 October 1991 the Minister for Finance decided to impose a general prohibition on financial intermediaries who offered investments in off-market commodities futures from cold calling potential clients.

9 According to the Netherlands Government, that decision was taken following numerous complaints received during 1991 by the Minister for Finance from investors who had made unfortunate investments in that sector. Since some of those complaints came from investors established in other Member States, he extended the prohibition to offers of services made to other Member States from the Netherlands, with a view to preserving the reputation of the Netherlands financial sector.

10 Those are the circumstances in which the Minister for Finance on 12 November 1991 prohibited Alpine Investments from contacting potential clients by telephone or in person unless those clients had first expressly authorized it in writing to contact them in such a manner.

11 Alpine Investments raised an administrative objection against the Minister’s decision prohibiting it from cold calling. Subsequently, the exemption having been replaced on 14 January 1992 by another exemption allowing it to place orders with another broker, Rodham & Renshaw Inc.,
an exemption which also included the prohibition of cold calling, it raised a new administrative objection on 13 February 1992.

12 By decision of 29 April 1992, the Minister for Finance rejected Alpine Investment's administrative objection. On 26 May 1992 Alpine Investments appealed to the Administrative Court.

13 Alpine Investments pleaded in particular that the prohibition of cold calling was incompatible with Article 59 of the Treaty in so far as it concerned potential clients established in Member States other than the Netherlands. The Administrative Court referred several questions on the interpretation of that provision to the Court of Justice:

"[(1) Must Article 59 of the EEC Treaty be interpreted as meaning that it also covers services which the provider offers by telephone from the Member State of his establishment to (potential) clients established in another Member State and therefore also provides from that Member State?]

(2) Does Article 59 also apply to the provisions and/or restrictions which in the Member State of establishment of the provider of services govern the lawful exercise of the occupation or business concerned but do not apply in any event not in the same way and to the same extent as to the exercise of that occupation or business in the Member State of establishment of (potential) recipients of the service in question and for that reason may constitute for the provider of services when offering his services to (potential) clients established in another Member State hindrances that do not apply to providers of similar services established in that other Member State?

If the answer to the second question is yes:

(3)(a) Can the concern to protect consumers and safeguard the reputation of the Netherlands securities trading sector which underlies a provision aimed at combating undesirable developments in the securities trading sector be regarded as imperative reasons of public interest justifying a hindrance such as that referred to in question (2)?

(b) Is a proviso in an exemption banning cold calling to be regarded as objectively necessary to protect the aforementioned concern and as proportionate to the objective pursued?"

14 It should be noted as a preliminary point that, were it applicable to transactions on commodities futures markets, Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field (OJ 1993 L 141, p. 27) post-dates the events which gave rise to the main proceedings.

Furthermore, Council Directive 85/577/EEC of 20 December 1985 concerning the protection of consumers in respect of contracts negotiated away from business premises (OJ 1985 L 372, p. 31) applies neither to contracts concluded by telephone nor to contracts for securities (Article 3(2)(e)).

15 The questions referred to the Court must therefore be examined solely in the light of the Treaty provisions on the freedom to provide services. It is common ground that, since they were provided for remuneration, the services provided by Alpine Investments are services covered by Article 60 of the EEC Treaty.

16 The national court's first and second questions essentially ask whether the prohibition of cold calling falls within the scope of Article 59 of the Treaty. If so, its third question asks whether that prohibition may nonetheless be justified.

The first question

17 There are two aspects to the national court's first question.

18 First, it asks whether the fact that the services in question are just offers without, as yet, an identifiable recipient of the service precludes application of Article 59 of the Treaty.

19 The freedom to provide services would become illusory if national rules were at liberty to restrict offers of services. The prior existence of an identifiable recipient cannot therefore be a condition for application of the provisions on the freedom to provide services.

20 The second aspect of the question is whether Article 59 covers services which the provider offers by telephone to persons established in another Member State and which he provides without moving from the Member State in which he is established.

21 In this case, the offers of services are made by a provider established in one Member State to a potential recipient established in another Member State. It follows from the express terms of Article 59 that there is therefore a provision of services within the meaning of that provision.

22 The answer to the first question is therefore that, on a proper construction, Article 59 of the EEC Treaty covers services which the provider offers by telephone to potential recipients established in other Member States and provides without moving from the Member State in which he is established.

The second question

23 The national court's second question asks whether rules of a Member State which prohibit providers of services established in its territory from making unsolicited telephone calls to potential clients established in other Member States in order to offer their services constitute a restriction on freedom to provide services within the meaning of Article 59 of the Treaty.

24 The preliminary observation should be made that the prohibition at issue applies to the offer of cross-border services.

25 In order to reply to the national court's question, three points must be examined in turn.

26 First, it must be determined whether the prohibition against telephoning potential clients in another Member State without their prior consent can constitute a restriction on freedom to provide services. The national court draws the Court's attention to the fact that providers established in the Member States where the potential recipients reside are not necessarily subject to the same prohibition or in any event not on the same terms.

27 A prohibition such as that at issue in the main proceedings does not constitute a restriction on freedom to provide services within the meaning of Article 59 solely by virtue of the fact that other Member States apply less strict rules to providers of similar services established in their territory (see the judgment in Case C-379/92 Peralta [1994] ECR I-3453, paragraph 48).

28 However, such a prohibition deprives the operators concerned of a rapid and direct technique for marketing and for contacting potential clients in other Member States. It can therefore constitute a restriction on the freedom to provide cross-border services.

29 Secondly, it must be considered whether that conclusion may be affected by the fact that the prohibition at issue is imposed by the Member State in which the provider is established and not by the Member State in which the potential recipient is established.

30 The first paragraph of Article 59 of the Treaty prohibits restrictions on freedom to provide services within the Community in general. Consequently, that provision covers not only restrictions laid down by the State of destination but also those laid down by the State of origin. As the Court has frequently held, the right freely to provide services may be relied on by an undertaking as against the State in which it is established if the services are provided for persons established in another Member State (see Case C-18/93 Corsica Ferries Italia v Corpo dei Piloti del Porto di Genova [1994] ECR I-1763, paragraph 30; Peralta, cited above, paragraph 40, and Case C-381/93 Commission v France [1994] ECR I-5145, paragraph 14).

31 It follows that the prohibition of cold calling does not fall outside the scope of Article 59 of the Treaty simply because it is imposed by the State in which the provider of services is established.
32 Finally, certain arguments adduced by the Netherlands Government and the United Kingdom must be considered. 33 They submit that the prohibition at issue falls outside the scope of Article 59 of the Treaty because it is a generally applicable measure, it is not discriminatory and neither its object nor its effect is to put the national market at an advantage over providers of services from other Member States. Since it affects only the way in which the services are offered, it is analogous to the non-discriminatory measures governing selling arrangements which, according to the decision in Joined Cases C-267 and 268/91 Keck and Mithouard [1993] ECR I-6097, paragraph 16, do not fall within the scope of Article 30 of the Treaty. 34 Those arguments cannot be accepted. 35 Although a prohibition such as the one at issue in the main proceedings is general and non-discriminatory and neither its object nor its effect is to put the national market at an advantage over providers of services from other Member States, it can none the less, as has been held above (see paragraph 28), constitute a restriction on the freedom to provide cross-border services. 36 Such a prohibition is not analogous to the legislation concerning selling arrangements held in Keck and Mithouard to fall outside the scope of Article 30 of the Treaty. 37 According to that judgment, the application to products from other Member States of national provisions restricting or prohibiting, within the Member State of importation, certain selling arrangements is not such as to trade between Member States so long as, first, those provisions apply to all relevant traders operating within the national territory and, secondly, they affect in the same manner, in law and in fact, the marketing of domestic products and of those from other Member States. The reason is that the application of such provisions is not such as to prevent access by the latter to the market of the Member State of importation or to impede such access more than it impeded access by domestic products. 38 A prohibition such as that at issue is imposed by the Member State in which the provider of services is established and affects not only offers made by him to addressees who are established in that State or move there in order to receive services but also offers made to potential recipients in another Member State. It therefore directly affects access to the market in services in the other Member States and is thus capable of hindering intra-Community trade in services. 39 The answer to the second question is therefore that rules of a Member State which prohibit providers of services established in its territory from making unsolicited telephone calls to potential clients established in other Member States in order to offer their services constitute a restriction on freedom to provide services within the meaning of Article 59 of the Treaty. 40 The third question 41 The national court’s third question asks whether imperative reasons of public interest justify the prohibition of cold calling and whether that prohibition must be considered to be objectively necessary and proportionate to the objective pursued. 42 The Netherlands Government argues that the prohibition of cold calling in off-market commodities futures trading seeks both to safeguard the reputation of the Netherlands financial markets and to protect the investing public. 43 Although the protection of consumers in the other Member States is not, as such, a matter for the Netherlands authorities, the nature and extent of that protection does none the less have a direct effect on the good reputation of Netherlands financial services. 44 Maintaining the good reputation of the national financial sector may therefore constitute an imperative reason of public interest capable of justifying restrictions on the freedom to provide financial services. 45 As for the proportionality of the restriction at issue, it is settled case-law that the measures imposed on the providers of services must be appropriate to achieve the intended aim and must not go beyond that which is necessary in order to achieve that objective (see Case C-288/89 Collective Antennevoorziening Gouda and Others v Commissariat voor de Media [1991] ECR I-4007, paragraph 15). 46 As the Netherlands Government has justifiably submitted, in the case of cold calling the individual, generally caught unawares, is in a position neither to ascertain the risks inherent in the type of transactions offered to him nor to compare the quality and price of the caller’s services with competitors’ offers. Since the commodities futures market is highly speculative and barely comprehensible for non-expert investors, it was necessary to protect them from the most aggressive selling techniques. 47 Alpine Investments argues however that the Netherlands Government’s prohibition of cold calling is not necessary because the Member State of the provider of services should rely on the controls imposed by the Member State of the recipient. 48 That argument must be rejected. The Member State from which the telephone call is made is best placed to regulate cold calling. Even if the receiving State wishes to prohibit cold calling or to make it subject to certain conditions, it is not in a position to prevent or control telephone calls from another Member State without the cooperation of the competent authorities of that State. 49 Consequently, the prohibition of cold calling by the Member State from which the telephone call is made, with a view to protecting investor confidence in the financial markets of that State, cannot be considered to be inappropriate to achieve the objective of securing the integrity of those markets. 50 Alpine Investments also argues that a general prohibition of telephone canvassing of potential clients is not necessary for the achievement of the objectives pursued by the Netherlands authorities. Requiring broking firms to tape-record unsolicited telephone calls made by them would suffice to protect consumers effectively. Such rules have moreover been adopted in the United Kingdom by the Securities and Futures Authority. 51 That point of view cannot be accepted. As the Advocate General correctly states in point 88 of his Opinion, the fact that one Member State imposes less strict rules than another Member State does not mean that the latter’s rules are disproportionate and hence incompatible with Community law. 52 Alpine Investments argues finally that, since it is of a general nature, the prohibition of cold calling does not take into account the conduct of individual undertakings and accordingly imposes an unnecessary burden on undertakings which have never been the subject of complaints by consumers. 53 That argument must also be rejected. Limiting the prohibition of cold calling to certain undertakings because of their past conduct might not be sufficient to achieve the objective of restoring and maintaining investor confidence in the national securities markets in general. 54 In any event, the rules at issue are limited in scope. First, they prohibit only the contacting of potential clients by telephone or in person without their prior agreement in writing, while other techniques for making contact are still permitted. Next, the measure affects relations with potential
clients but not with existing clients who may still give their written agreement to further calls. Finally, the prohibition of unsolicited telephone calls is limited to the sector in which abuses have been found, namely the commodities futures market.

55 In the light of the above, the prohibition of cold calling does not appear disproportionate to the objective which it pursues.

56 The answer to the third question is therefore that Article 59 does not preclude national rules which, in order to protect investor confidence in national financial markets, prohibit the practice of making unsolicited telephone calls to potential clients resident in other Member States to offer them services linked to investment in commodities futures.

Decision on costs

Costs

57 The costs incurred by the Belgian, Netherlands and Greek Governments, the United Kingdom and the Commission of the European Communities, which have submitted observations to the Court, are not recoverable. Since these proceedings are, for the parties to the main proceedings, a step in the proceedings pending before the national court, the decision on costs is a matter for that court.

Relevant Case-Law on Online Betting and Online Games of Chance

C-258/08 Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator

JUDGMENT OF THE COURT (Second Chamber)

1 This reference for a preliminary ruling concerns the interpretation of Article 49 EC.

2 The reference has been made in proceedings between the Stichting de Nationale Sporttotalisator, a foundation governed by Netherlands law (‘De Lotto’), and Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd, companies established in the United Kingdom (‘the Ladbrokes companies’), concerning the possibly unlawful conduct of those companies on the Netherlands market for games of chance.

Legal context

3 Article 1 of the Law on games of chance [Wet op de kansspelen; ‘the Wok’] provides:

(a) providing an opportunity to compete for prizes if the winners are designated by means of any calculation of probability over which the participants are generally unable to exercise a dominant influence, unless a licence therefor has been granted pursuant to this Law;

(b) promoting participation either in an opportunity as referred to under (a), provided without a licence pursuant to this Law, or in a similar opportunity, provided outside the Kingdom of the Netherlands in Europe, or to maintain a stock of materials intended to publicise or disseminate knowledge of such opportunities;’

4 Article 16 of the Wok is worded as follows:

‘1. The Minister for Justice and the Minister for Welfare, Public Health and Culture may grant to one legal person with full legal capacity a licence, for a period to be determined by them, to organise sports-related prize competitions in the interests of bodies operating for public benefit, particularly in the area of sport and physical education, culture, social welfare and public health.

2. The proceeds from prize competitions … shall be applied in respect of the interests which the legal person intends to serve by organising and operating sports-related prize competitions.

3. At least 47.5% of total proceeds from games of chance organised pursuant to this Title and to Title IVa, to be calculated on the basis of a calendar year, shall be allocated to the distribution of prizes.’

5 Article 21 of the Wok states:

1. The Ministers referred to in Article 16 shall lay down rules concerning licences for the organisation of sports-related prize competitions.

2. Those rules relate, inter alia to:

a. the number of competitions to be organised;

b. the method of determining results and the prize scheme;

c. the management and covering of organisational costs;

d. the allocation of revenue from competitions organised;

e. the constitution and regulations of the legal person;

f. monitoring of compliance with the legislation by the authorities;

g. delivery and publication of the report to be drawn up annually by the legal person concerning its activities and financial results.’

6 The dispute in the main proceedings and the questions referred for a preliminary ruling

6 Netherlands legislation in relation to games of chance is based on a system of exclusive licences under which (i) the organisation or promotion of games of chance is prohibited unless an administrative licence for that purpose has been issued, and (ii) only one licence is granted by the national authorities in respect of each of the games of chance authorised.

7 Furthermore, it is apparent from the case-file in the main proceedings as supplied to the Court by the referring court that there is no possibility at all of offering games of chance interactively via the internet in the Netherlands.

Operative part

On those grounds,

THE COURT,

in answer to the questions referred to it by the College van Beroep voor het Bedrijfsleven by order of 28 April 1993, hereby rules:

1. On a proper construction, Article 59 of the EEC Treaty covers services which the provider offers by telephone to potential recipients established in other Member States and provides without moving from the Member State in which he is established.

2. Rules of a Member State which prohibit providers of services established in its territory from making unsolicited telephone calls to potential clients established in other Member States in order to offer their services constitute a restriction on freedom to provide services within the meaning of Article 59 of the Treaty.

3. Article 59 does not preclude national rules which, in order to protect investor confidence in national financial markets, prohibit the practice of making unsolicited telephone calls to potential clients resident in other Member States to offer them services linked to investment in commodities futures.
8 De Lotto is a non-profit-making foundation governed by private law which holds a licence for the organisation of sports-related prize competitions, the lottery and numbers games. Its objects, according to its constitution, are the collection of funds by means of the organisation of games of chance and the distribution of those funds among institutions working in the public interest, particularly in the fields of sport, physical education, general welfare, public health and culture.

The Ladbrokes companies are engaged in the organisation of sports-related prize competitions and are particularly well known for their bookmaking business. They offer a number of mainly sports-related games of chance on their internet site. They also offer the possibility of participating via a freephone number in the betting activities which they organise. The companies do not physically carry on any activity in the Netherlands.

10 De Lotto alleged that the Ladbrokes companies were, via the internet, offering games of chance to persons residing in the Netherlands for which they did not have the requisite licence under the Wok, and made an application for interim relief before the Rechtbank Arnhem (District Court, Arnhem) for the Ladbrokes companies to be required to put an end to that activity.

[...]

13 The Hoge Raad der Nederlanden took the view that an interpretation of European Union law was required to enable it to determine the dispute before it, and decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) Does a restrictive national gaming policy which is aimed at channelling the propensity to gamble and which in fact contributes to the achievement of the objectives pursued by the national legislation in question, namely the curbing of gambling addiction and the prevention of fraud, inasmuch as, by reason of the regulated offer of games of chance, participation in gambling activities occurs on a (much) more limited scale than would be the case if there were no national regulatory system, satisfy the condition set out in the case-law of the Court of Justice of the European Communities, particularly in the judgment in Case C-243/01 Gambelli and Others [2003] ECR I-13031, that such restrictions must limit betting activities in a consistent and systematic manner, even where the licence-holder/s is/are permitted to make the games of chance which they offer attractive by introducing new games, to bring the games which they offer to the notice of a wide public by means of advertising and thereby to keep (potential) gamblers away from the unlawful offer of games of chance [see Joined Cases C-338/04, C-359/04 and C-360/04 Placanica and Others [2007] ECR I-1891, paragraph 55, in fine)?

(2) (a) Assuming that national legislation governing gaming policy is compatible with Article 49 EC, is it for the national courts to determine, on every occasion on which they apply that legislation in practice in an actual case, whether the measure to be imposed, such as an order that a particular website be made inaccessible to residents of the Member State concerned by means of software designed for that purpose, in order to prevent them from participating in the games of chance offered thereon, in itself and as such satisfies the condition, in the specific circumstances of the case, that it should actually serve the objectives which might justify the national legislation in question, and whether the restriction resulting from that legislation and its application on the freedom to provide services is not disproportionate in the light of those objectives?

(b) In answering Question 2a, does it make any difference if the measure to be implemented is not ordered and imposed in the context of the application of the national legislation by the authorities, but in the context of a civil action in which an organiser of games of chance operating with the required licence requests imposition of the measure on the ground that an unlawful act has been committed in its regard under civil law, inasmuch as the opposing party contravened the national legislation in question, thereby gaining an unfair advantage over the party operating with the required licence?

(3) Should Article 49 EC be interpreted in such a way that the application of that article results in the competent authority of a Member State being unable, on the basis of the closed licensing system that exists in that State for the provision of gambling services, to prohibit a service provider which has already been granted a licence in another Member State for the online provision of such services from also offering those services online in the first Member State?

Consideration of the questions referred
The first question

14 By its first question, the national court asks, in essence, whether national legislation such as that at issue in the main proceedings, which seeks to curb addiction to games of chance and to combat fraud, and which in fact contributes to the achievement of those objectives, can be regarded as limiting betting activities in a consistent and systematic manner even where the holder(s) of an exclusive licence are entitled to make what they are offering on the market attractive by introducing new games and by means of advertising.

15 Article 49 EC requires the abolition of all restrictions on the freedom to provide services, even if those restrictions apply without distinction to national providers of services and to those from other Member States, when they are liable to prohibit, impede or render less advantageous the activities of a service provider established in another Member State where it lawfully provides similar services. The freedom to provide services is for the benefit of both providers and recipients of services [Case C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International [2009] ECR I-0000, paragraph 51 and the case-law cited].

16 It is common ground that the legislation of a Member State under which exclusive rights to organise and promote games of chance are conferred on a single operator, and which prohibits any other operator, including an operator established in another Member State, from offering via the internet services within the scope of that regime in the territory of the first Member State, constitutes a restriction on the freedom to provide services enshrined in Article 49 EC [Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 52, and Case C-203/08 Sporting Exchange [2010] ECR I-0000, paragraph 24].

17 However, it is necessary to assess whether such a restriction may be allowed as a derogation expressly provided for by Articles 45 EC and 46 EC, applicable in this area by virtue of Article 55 EC, or justified, in accordance with the case-law of the Court, by overriding reasons in the public interest (see, to that effect, Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 55).

18 Article 46(1) EC allows restrictions justified on grounds of public policy, public security or public health. A certain number of overriding reasons in the public interest which may also justify such restrictions have been recognised by the case-law of the Court, including, in particular, the objectives of consumer protection and the prevention of both fraud and incitement to squander money on gambling, as well as the general need to preserve public order [Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 56].

19 In that context, moral, religious or cultural factors, as well as the morally and financially harmful consequences for the individual and for society associated with betting and gaming, may serve to justify a margin of discretion for the national authorities, sufficient to enable them to determine what is required in order to ensure consumer protection and the preservation of public order (Gambelli and Others, paragraph 63, and Placanica and Others, paragraph 47).
20 The Member States are free to set the objectives of their policy on betting and gambling according to their own scale of values and, where appropriate, to define in detail the level of protection sought. The restrictive measures that they impose must, however, satisfy the conditions laid down in the case-law of the Court, in particular as regards their proportionality (see, to that effect, Placanica and Others, paragraph 48, and Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 59).

21 Specifically, restrictions based on the reasons referred to in paragraphs 19 to 20 of the present judgment must be suitable for achieving those objectives, inasmuch as they must serve to limit betting activities in a consistent and systematic manner (see, to that effect, Gambelli and Others, paragraph 67).

22 According to the case-law of the Court, it is for the national courts to determine whether Member States’ legislation actually serves the objectives which might justify it and whether the restrictions it imposes do not appear disproportionate in the light of those objectives (Gambelli and Others, paragraph 75, and Placanica and Others, paragraph 58).

23 In the present case, the wording of the first question put by the referring court shows that the objectives of the Wok are clearly identified by that court, namely protection of consumers by the curbing of addiction to games of chance and prevention of fraud, and that, in the referring court’s view, the national legislation at issue in the main proceedings does in fact serve those objectives and does not go beyond what is required in order to achieve them.

24 The referring court nevertheless has doubts as to the consistent and systematic nature of the national legislation, since the legislation pursues the objectives referred to in the preceding paragraph while allowing actual gambling operators who have exclusive rights to organise games of chance in the Netherlands, such as De Lotto, to offer new games and to use advertising to make what they are offering on the market attractive.

25 As the Court has already held, it is possible that a policy of controlled expansion in the betting and gaming sector may be entirely consistent with the objective of drawing players away from clandestine betting and gambling – and, as such, activities which are prohibited – to activities which are authorised and regulated. In order to achieve that objective, authorised and regulated operators must represent a reliable, but at the same time attractive, alternative to a prohibited activity. This may as such necessitate the offer of an extensive range of games, advertising on a certain scale and the use of new distribution techniques (Placanica and Others, paragraph 58).

26 While it is true that the grounds of the judgment in Placanica and Others refer solely to the objective of crime prevention in the betting and gaming sector, whereas, in the present case, the Netherlands legislation is also designed to curb gambling addiction, the fact remains that those two objectives must be considered together, since they relate both to consumer protection and to the preservation of public order (see, to that effect, Case C-275/92 Schindler [1994] ECR I-1039, paragraph 58; Case C-124/97 Lárra and Others [1999] ECR I-6067, paragraph 33; and Case C-67/98 Zenatti [1999] ECR I-7289, paragraph 31).

27 It is for the national court to determine, in the light of the facts of the dispute before it, whether, in so far as the national legislation at issue in the main proceedings allows the holders of an exclusive licence to offer new games and to advertise, it may be regarded as forming part of a policy of controlled expansion in the betting and gaming sector, aiming, in fact, to channel the propensity to gamble into activities that are lawful.

28 If it were established that the Kingdom of the Netherlands is pursuing a policy of substantially expanding betting and gaming, by excessively inciting and encouraging consumers to participate in such activities, principally with a view to obtaining funds, and that, for that reason, the financing of social activities through a levy on the proceeds of authorised games of chance constitutes not an incidental beneficial consequence but the real justification for the restrictive policy adopted by that Member State, it would have to be concluded that such a policy does not limit betting and gaming activities in a consistent and systematic manner and is not, therefore, suitable for achieving the objective of curbing consumer addiction to such activities.

29 In the context of that assessment, it is, specifically, for the national court to determine whether unlawful gaming activities may constitute a problem in the Netherlands and whether the expansion of authorised and regulated activities would be likely to solve such a problem.

30 Since the objective of protecting consumers from gambling addiction is, in principle, difficult to reconcile with a policy of expanding games of chance characterised, inter alia, by the creation of new games and by the advertising of such games, such a policy cannot be regarded as being consistent unless the scale of unlawful activity is significant and the measures adopted are aimed at channelling consumers’ propensity to gamble into activities that are lawful.

31 The fact that demand for games of chance in the Netherlands has already increased noticeably, particularly at a clandestine level – assuming that is established as De Lotto indicated at the hearing – must be taken into consideration.

32 The national legislation at issue in the main proceedings aims not only to combat fraud and other crimes in the sphere of games of chance, but also to safeguard consumer protection. Thus, a fair balance has to be drawn between demand for the controlled expansion of authorised games of chance with the aim of making the provision of such games attractive for the public and the need to reduce as far as possible consumer addiction to such games.

33 Some of the evidence in the case-file submitted to the Court may be relevant for the purposes of that assessment.

34 According to the terms of the 2004 decision in relation to De Lotto’s exclusive licence to organise sports-related price competitions, that foundation shall ensure that marketing and advertising activities are sensible and balanced in content, and shall seek, in particular, to combat disproportionate participation in games of chance organised pursuant to the present decision.

35 Furthermore, by letter of 23 June 2004, the Netherlands Minister for Justice requested that licensees ‘severely restrict the amount of advertising and give shape and substance to that restrictive policy on advertising by drawing up a code of conduct and on advertising for operators of games of chance that is to be applicable to all of them’. That code came into force in the Netherlands on 15 February 2006.

36 That evidence may establish an intention on the part of the national authorities narrowly to circumscribe the expansion of games of chance in the Netherlands.

37 However, it is for the national court to determine whether the development of the market for games of chance in the Netherlands is such as to demonstrate that the expansion of games of chance is being supervised effectively by the Netherlands authorities, both with regard to the scale of advertising undertaken by holders of exclusive licences and with regard to the latter’s creation of new games, and, in consequence, to reconcile appropriately the simultaneous achievement of the objectives pursued by the national legislation.

38 In the light of the foregoing considerations, the answer to the first question is that national legislation, such as that at issue in the main proceedings, which seeks to curb addiction to games of chance and to combat fraud, and which in fact contributes to the achievement of those objectives, can be regarded as limiting betting activities in a consistent and systematic manner even where the holder(s) of an exclusive licence is entitled to make what they are offering on the market attractive by introducing new games and by means of advertising. It is for the national court to determine
whether unlawful gaming activities constitute a problem in the Member State concerned which might be solved by the expansion of authorised and regulated activities, and whether that expansion is on such a scale as to make it impossible to reconcile with the objective of curbing such addiction.

The second question

39 By its second question, the national court asks, in essence, whether, for the purpose of applying legislation of a Member State on games of chance which is compatible with Article 49 EC, it is for the national courts to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality. The national court also asks whether it makes any difference if the measure to be taken is required not by the public authorities but by an individual in the context of a civil action.

40 As stated in paragraph 22 of the present judgment, it is for the national courts to determine whether Member States’ legislation which restricts a fundamental freedom enshrined in the Treaty is suitable for achieving the public interest objectives that might justify it, and whether the restrictions it imposes do not appear disproportionate in the light of those objectives.

41 The wording of the second question is based on the premise that the Netherlands legislation on games of chance is compatible with Article 49 EC.

42 In the case at issue in the main proceedings, the restriction on the freedom to provide services enshrined in Article 49 EC derives directly from the provisions of the Wok, in so far as, under the latter, exclusive rights to organise and promote games of chance are conferred on a single operator and any other operator, including an operator established in another Member State, is prohibited from offering via the internet services within the scope of that regime in the territory of the Member State concerned.

43 A measure which implements the national legislation at issue in the main proceedings, such as the injunction which the judge who heard the application for interim relief imposed on the Ladbrokes companies in order to block access to their internet site for persons residing in the Netherlands and to make it impossible for such persons to participate in telephone betting, is an indispensable element of the protection in respect of games of chance that is intended to be provided by the Netherlands within its own territory and cannot, therefore, be regarded as an additional restriction over and above that which arises directly from the provisions of the Wok.

44 That implementing measure merely ensures the effectiveness of Netherlands legislation concerning games of chance. Without such a measure, the prohibition laid down by the Wok would be ineffective, since economic operators who are not licensed by the national authorities would be able to provide games of chance on the Netherlands market.

45 Since the implementing measure laid down by the national legislation does not, in itself, impose additional restrictions on the market, consideration of its conformity with European Union law is closely linked to the national court’s examination of the compatibility of the Wok with Article 49 EC.

46 In those circumstances, contrary to what is submitted by the Ladbrokes companies, there is no further need to consider whether the implementing measure is actually justified by an overriding reason in the public interest, whether it is suitable for achieving the objectives of limiting addition to gambling and preventing fraud or whether it does not go beyond what is necessary to achieve those objectives.

47 Moreover, whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

48 The subject-matter of that dispute concerns the application of Article 49 EC, which confers on individuals rights which are enforceable by them and which the national courts must protect (see Case 33/74 van Binsbergen [1974] ECR 1299, paragraph 27, and Case C: 208/05 ITC [2007] ECR I-181, paragraph 67).

49 It is for the national courts, irrespective of the procedure by which the matter has been brought before them, to take any measures necessary to ensure that economic operators exercise their freedom to provide services in a Member State and in situations falling within the scope of European Union law.

50 It follows from the foregoing observations that the answer to the second question is that, for the purpose of applying legislation of a Member State on games of chance which is compatible with Article 49 EC, the national courts are not required to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality, in so far as that measure is necessary to ensure the effectiveness of that legislation and does not include any additional restriction over and above that which arises from the legislation itself. Whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

The third question

51 By its third question, the national court asks, in essence, whether Article 49 EC must be interpreted as precluding legislation of a Member State, such as the legislation at issue in the main proceedings, under which exclusive rights to organise and promote games of chance are conferred on a single operator, and which prohibits any other operator, including an operator established in another Member State, from offering via the internet services within the scope of that regime in the territory of the first Member State.

52 That question falls within the same legal framework as the first question referred to the case giving rise to the judgment in Sporting Exchange and is identical to it.

53 The Ladbrokes companies submit that they are holders of a licence issued by the authorities of the United Kingdom of Great Britain and Northern Ireland which allows them to offer sports-related prize competitions and other games of chance via the internet and by telephone, and are subject in the United Kingdom to very strict legislation for the prevention of fraud and of addiction to games of chance. They also allege that, where a Member State imposes restrictions relating to the organisation of such games, it must take into account the fact that the public interest justifying the restriction in question is already protected by the rules laid down by the Member State in which the provider of services is licensed to operate such games. There should be no duplication of controls and safeguards.

54 In that regard, it should be noted that the internet gaming industry has not been the subject of harmonisation within the European Union. A Member State is therefore entitled to take the view that the mere fact that an operator such as the Ladbrokes companies lawfully offers services in that sector via the internet in another Member State, in which it is established and where it is in principle already subject to statutory conditions and controls on the part of the competent authorities in that State, is not a sufficient assurance that national consumers will be protected against the risks of fraud and crime, in the light of the difficulties liable to be encountered in such a context by the authorities of the Member State of establishment in assessing the
55 In addition, because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators against consumers compared with the traditional markets for such games (Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 70).

56 The fact that an operator who offers games of chance via the internet does not pursue an active sales policy in the Member State concerned, particularly because he is not making use of advertising in that State, cannot be regarded as running counter to the considerations set out in the two preceding paragraphs. Those considerations are based solely on the effects on the mere accessibility of games of chance via the internet and not on the potentially different consequences of the active or passive provision of services by that operator.

57 It follows from this that, in the light of the specific features associated with the provision of games of chance via the internet, the restriction at issue in the main proceedings may be regarded as justified by the objective of combating fraud and crime (see, to that effect, Liga Portuguesa de Futebol Profissional and Bwin International, paragraph 72).

58 Therefore, the answer to the third question is that Article 49 EC must be interpreted as not precluding legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

3. For the purpose of applying legislation of a Member State on games of chance which is compatible with Article 49 EC, the national courts are not required to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality, in so far as that measure is necessary to ensure the effectiveness of that legislation and does not include any additional restriction over and above that which arises from the legislation itself. Whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

59 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Second Chamber) hereby rules:

1. National legislation, such as that at issue in the main proceedings, which seeks to curb addiction to games of chance and to combat fraud, and which in fact contributes to the achievement of those objectives, can be regarded as limiting betting activities in a consistent and systematic manner even where the holder(s) of an exclusive licence are entitled to make what they are offering on the market attractive by introducing new games and by means of advertising. It is for the national court to determine whether unlawful gaming activities constitute a problem in the Member State concerned which might be solved by the expansion of authorised and regulated activities, and whether that expansion is on such a scale as to make it impossible to reconcile with the objective of curbing such addiction.

2. Article 49 EC must be interpreted as not precluding legislation of a Member State on games of chance which is compatible with Article 49 EC, the national courts are not required to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality, in so far as that measure is necessary to ensure the effectiveness of that legislation and does not include any additional restriction over and above that which arises from the legislation itself. Whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

3. Article 49 EC must be interpreted as not precluding legislation of a Member State on games of chance which is compatible with Article 49 EC, the national courts are not required to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality, in so far as that measure is necessary to ensure the effectiveness of that legislation and does not include any additional restriction over and above that which arises from the legislation itself. Whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or of an application by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court.

Costs

Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

Relevant Case-Law on Payment Instruments and Payment Cards

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE
COMP/34.579 — MasterCard, Case COMP/36.518 —
EuroCommerce, Case COMP/38.580 — Commercial Cards

Text with EEA relevance

relating to a proceeding under Article 81 of the EC Treaty
and Article 53 of the EEA Agreement (2009/C 264/04,
notified under document C(2007) 6474)

(Only the English text is authentic)

On 19 December 2007, the Commission adopted a decision relating to a proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement (the Decision). In accordance with the provisions of Article 30 of Council Regulation (EC) No 1/2003 [1], the Commission herewith publishes the names of the parties and the main content of the Decision, having regard to the legitimate interest of undertakings in the protection of their business interests. A non-confidential version of the Decision is available on the

Directorate-General for Competition’s website at the following address:
http://europa.eu.int/comm/competition/antitrust/cases/index/

1. INTRODUCTION

(1) The Decision finds that the MasterCard payment organisation and the entities representing it, that is MasterCard Incorporated, MasterCard International Incorporated and MasterCard Europe SPRL, have infringed Article 81 of the Treaty and Article 53 of the EEA Agreement by in effect setting a minimum price merchants must pay to their acquiring bank for accepting payment cards in the European Economic Area, by means of the Intra-EEA fallback interchange fees for MasterCard branded consumer credit and charge cards and for MasterCard or Maestro branded debit cards.

2. CASE DESCRIPTION

2.1. The proceedings

(2) The procedure was initiated on the basis of a complaint submitted on 30 March 1992 by the British Retail Consortium (BRC), a trade association representing UK
retailers. In its complaint the BRC alleged that each of Europay International SA and Visa restricted competition by its arrangements on cross-border interchange fees.

(3) The BRC complaint was withdrawn when a similar complaint was filed by EuroCommerce, a retail, wholesale and international trade representation in the European Union, on 23 May 1997. This complaint addresses certain practices and rules of MasterCard and Visa, in particular multilaterally agreed interchange fees.

(4) In the time between 22 May 1992 and 1 July 1995, Europay notified the network rules of the Europay payment card association including those on multilateral interchange fees.

(5) On 22 November 2002 the Commission opened an ex-officio investigation regarding Visa’s and MasterCard’s respective intra-EEA interchange fees for commercial cards.

(6) On 25 July 2003 MasterCard informed the Commission of its intention to initiate proceedings under Article 232 of the EC Treaty (failure to act) unless the Commission took a formal position with respect to MasterCard’s intra-EEA interchange fees.

(7) On 24 September 2003 and 21 June 2006 the Commission sent two Statements of Objections to MasterCard Europe SPRIL, the legal successor of Europay, as well as to MasterCard International Inc. and MasterCard Incorporated addressing the organisation’s network rules and decisions on intra-EEA interchange fees.

(8) On 27 November 2005 MasterCard exercised its right to be heard in an oral hearing. The hearing was also attended by EuroCommerce and nine third parties.

(9) On 23 March 2007 the Commission sent a letter to MasterCard (letter of facts) providing MasterCard with access to documents collected since MasterCard had access to the file in July and August 2006 and setting out possible conclusions the Commission intended to draw from the new facts in the Decision.

(10) On 13 December 2007 the Advisory Committee gave a favourable opinion on the draft Commission Decision.

2.2. The facts

(11) MasterCard operates an international “open” or “four-party” point of sales (POS) payment system. MasterCard’s payment cards system enables consumers to use plastic cards for payment transactions at POS, which is — most often — a payment terminal in a merchant outlet. Such a system involves five main groups of players: (i) cardholders; (ii) merchants; (iii) the scheme owner (here: MasterCard); (iv) card issuing banks; and (v) acquiring banks. Issuers issue cards to cardholders and acquirers recruit merchants for payment card acceptance.

(12) The Decision deals with MasterCard’s network rules and decisions of its member bank Mandates and the organisation’s management on Intra-EEA fallback interchange fees and SEPA fallback interchange fees. These multilateral interchange fees (MIFs) are retained for each payment card transaction. Under the MasterCard organisation’s network rules the acquiring banks pay interchange fees to the issuing banks. When the cardholder uses his or her card to buy from the merchant, the merchant receives from the acquiring bank the retail price less a merchant service charge. The issuing bank pays the acquiring bank the retail price minus an interchange fee. In addition to the interchange fee from the acquiring bank, the issuing bank receives from the customer the value of the payment plus any annual fee, any interest payment on debt outstanding, late payment fees, etc.

(13) Intra-EEA fallback interchange fees and SEPA fallback interchange fees apply to cross-border card payments in the European Economic Area (EEA) and domestic card payments within several Member States of the EEA with MasterCard or Maestro branded payment cards. The fees are “fallback” fees in the sense that they are only charged in the absence of specific bilateral agreements between an issuing and an acquiring bank on interchange fees.

3. LEGAL ASSESSMENT

Article 81(1) of the Treaty

(14) The MIF in MasterCard’s scheme restricts competition between acquiring banks by inflating the base on which acquiring banks set charges to merchants and thereby setting a floor under the merchant fee. In the absence of the multilateral interchange fee the merchant fees set by acquiring banks would be lower.

(15) The MasterCard’s European Board (…) [**] and/or the Global Board (…) [**] decisions on the level and structure of Intra-EEA fallback interchange fees and the related network rules adopted by the Global Board of MasterCard International Inc. are decisions of an association of undertakings within the meaning of Article 81(1) of the Treaty. They remain decisions of an association also after the Initial Public Offering (IPO) of MasterCard Incorporated on 25 May 2006 and the related changes in the governance of the payment organisation in Europe with regard to the authority for setting the level of multilateral fallback interchange fees. The member banks of the MasterCard payment organisation agreed to the IPO and the ensuing changes in the organisation’s governance in order to perpetuate the MIF as part of the business model in a form which they perceived to be less exposed to antitrust scrutiny. Even after the IPO of MasterCard Incorporated interchange fees in the MasterCard organisation are not “unilaterally imposed”. MasterCard’s member banks still share a common interest because the MIF yields guaranteed revenues for their issuing business. There is thus a continuing commonality of the banks’ interests in a MIF after the IPO which is also reflected in the setting of interchange fee rates by MasterCard (…) [**]. In setting interchange fee rates the Global Board cannot ignore the commercial interests of the banks without whom the system would not function, because it yields guaranteed revenues for their issuing business.

(16) An open payment card scheme such as MasterCard’s can operate without a MIF as is evidenced by the existence of comparable open payment card schemes without a MIF. Article 81(3) of the Treaty

(17) The conditions set out in Article 81(3) EC for an exemption from the prohibition of Article 81(1) EC are not fulfilled.

(18) In relation to the first condition of Article 81(3) (contribution to technical or economic progress), MasterCard has failed to demonstrate a causal link between its MIF and objective efficiencies. MasterCard alleges that the central efficiency of its MIF is to help the scheme to maximise system output by balancing cardholder and merchant demands.

(19) The Commission does not dispute in general that payment systems are characterised by indirect network externalities and that in theory a revenue transfer between issuing and acquiring banks may help optimise the utility of the network to its users. However, whether a collectively fixed interchange fee should flow from acquirers to issuers or vice versa, and at which level it should be set cannot be determined in a general manner by economic theory alone, as theories always rely on assumptions that may not sufficiently reflect market reality. Rather, any claim that a MIF creates efficiencies within the first condition of Article 81(3) of the Treaty must be founded on a detailed, robust and compelling analysis that relies in its assumptions and deductions on empirical data and facts. MasterCard in particular failed to provide empirical evidence for its central claim that the MIF maximises the scheme’s "output" and for a causal link to other objective efficiencies claimed. It was therefore not established that the restrictive effects of the MIF in the acquiring markets are duly offset by objective efficiencies. Despite repeated requests by the Commission MasterCard failed to submit any empirical evidence on the positive effects of its MIF on system output and related efficiencies.
The Commission does not share MasterCard’s view that the competitive process and market forces automatically lead to a MIF that can safely be assumed to be efficiency enhancing. Neither the forces of inter-system competition nor acquiring banks or merchants exert sufficient constraints on the body in charge of setting the MIF in the MasterCard organisation.

(21) The specific framework underlying MasterCard’s MIF is a model written by William Baxter in 1983. This model is, however, severely limited by the fact that it takes consumer and merchant demand as given in that neither strategically reacts to possible actions by the other. The Baxter model also relies on the unrealistic assumption that there is no variation in the benefits that merchants perceive from accepting cards, in other words it regards merchants as homogeneous. Baxter’s result finally relies on the unrealistic assumption of a perfectly competitive banking industry.

(22) Moreover, the methodologies used by MasterCard for implementing this framework in practice are unconvincing as they do not sufficiently reflect the underlying theory. The methodologies suffer from considerable shortcomings as they establish an imbalance between card issuing and merchants acquiring solely on the basis of cost considerations while omitting to consider the banks’ revenues, as well. Moreover, contrary to the merchant demand analysis, MasterCard does not even attempt to quantify the willingness to pay of cardholders and simply assumes the relative unwillingness of this customer group to pay for the convenience of using payment cards. There are also doubts as to the usefulness of MasterCard’s proxy for quantifying the willingness to pay of merchants in the credit card segment.

(23) Under the second condition of Article 81(3) of the Treaty, the MasterCard payment organisation of 3.5 % of MasterCard Incorporated’s global turnover in the preceding business year. This penalty will be calculated as from the first day after the infringed order takes effect.

(32) The MasterCard payment organisation and the legal entities representing it shall bring to an end the infringement by formally repealing its intra-Eurozone fallback interchange fees within 6 months upon notification of the Decision. They shall moreover modify the association’s network rules to reflect the Commission Decision. They shall repeal all decisions taken by MasterCard’s European Board and/or by MasterCard’s Global Board (…) [*] on Intra-EAA fallback interchange fees and on Intra-Eurozone fallback interchange fees.

(33) Within 6 months after notification of this Decision the legal entities representing the MasterCard payment organisation shall communicate all changes of the association’s network rules and the repeal of decisions to all financial institutions holding a license for issuing and/or acquiring in the MasterCard payment organisation in the European Economic Area and to all clearing houses and settlement banks which clear and/or settle POS payment card transactions in the MasterCard payment organisation in the European Economic Area.

(34) If the legal entities representing the MasterCard payment organisation fail to comply with any of the orders set out in the Decision, the Decision imposes a daily penalty payment on the legal entities representing the MasterCard payment organisation of 3.5 % of MasterCard Incorporated’s daily consolidated global turnover in the preceding business year according to Article 24(3)(a) of Regulation (EC) No 1/2003. This penalty will be calculated as from the first day after the infringed order takes effect.


[**] Business secret — information pertaining to MasterCard’s interchange fee rules and procedure for determining the level of the interchange fee.
JUDGMENT OF THE COURT (Grand Chamber)
23 April 2013 (*)

In Joined Cases C-478/11 P to C-482/11 P, Five APPEALS under Article 56 of the Statute of the Court of Justice of the European Union, brought on 21 September 2011, Laurent Gbagbo (C-478/11 P), Katinan Justin Koné (C-479/11 P), Akissi Danièle Boni-Claverie (C-480/11 P), Alcide Dédjé (C-481/11 P) and Affi Pascal N’Guessan (C-482/11 P) v Council of the European Union


2 On 15 November 2004 the United Nations Security Council adopted Resolution 1572 (2004) in which it declared, inter alia, that the situation in Côte d’Ivoire continued to pose a threat to international peace and security in the region and decided to impose certain restrictive measures against that country.

3 Paragraph 14 of Resolution 1572 (2004) established a committee (‘the Sanctions Committee’) whose tasks included the designation of persons and entities to be subject to the restrictive measures in respect of travel and freezing of funds, financial assets and economic resources imposed by paragraphs 9 and 11 of that resolution and the regular updating of the list of persons and entities.

4 On 13 December 2004 the Council of the European Union, considering that action by the European Community was necessary in order to implement Resolution 1572 (2004), adopted Common Position 2004/852/CFSP concerning restrictive measures against Côte d’Ivoire (OJ 2004 L 368, p. 50).

5 On 12 April 2005, since it took the view that a regulation was necessary in order to implement, at Community level, the measures described in Common Position 2004/852, the Council adopted Council Regulation (EC) No 560/2005 of 12 April 2005 imposing certain specific restrictive measures directed against certain persons and entities in view of the situation in Côte d’Ivoire (OJ 2005 L 95, p. 1).

6 Common Position 2004/852 was extended and amended on several occasions, before being repealed and replaced by Council Decision 2010/656/CFSP of 29 October 2010 renewing the restrictive measures against Côte d’Ivoire (OJ 2010 L 285, p. 28).

7 An election for the office of President of the Republic of Côte d’Ivoire was held on 31 October and 28 November 2010.

8 On 3 December 2010 the Special Representative of the United Nations Secretary General for Côte d’Ivoire certified the final result of the second round of the presidential election, as declared by the president of the independent electoral commission on 2 December 2010, confirming the victory of Mr Alassane Ouattara in the Presidential election.

9 On 13 December 2010 the Council emphasised the importance of the Presidential election held on 31 October and 28 November 2010 for the return of peace and stability in Côte d’Ivoire and declared it to be imperative that the sovereign wish expressed by the Ivorian people be respected. The Council also noted the conclusions of the Special Representative of the United Nations Secretary General for Côte d’Ivoire as part of his task of certification and congratulated Mr Ouattara on his election as President of the Republic of Côte d’Ivoire.

10 On 17 December 2010 the European Council called on all Ivorian leaders, both civilian and military, who had not yet done so, to place themselves under the authority of the democratically elected President, Mr Ouattara. The European Council confirmed the determination of the European Union to take targeted measures against those who might continue to obstruct respect of the sovereign wish expressed by the Ivorian people.


12 Article 4(1) of Decision 2010/656, as amended by Decision 2010/801, reads as follows:

‘Member States shall take the necessary measures to prevent the entry into, or transit through, their territories of:
(a) the persons referred to in Annex I and designated by the Sanctions Committee;
(b) the persons referred to in Annex II who are not included in the list in Annex I and who are obstructing the process of peace and national reconciliation, and in particular who are jeopardising the proper outcome of the electoral process.’

13 The names of Mr Gbagbo and Mr N’Guessan were, by means of Decision 2010/801, included in the list in Annex II to Decision 2010/656, as amended by Decision 2010/81.

14 On 11 January 2011 the Council adopted Decision 2011/17/CFSP in order to enter, in view of the gravity of the situation in Côte d’Ivoire, the names of additional persons in the list in Annex II to Decision 2010/656, as amended by Decision 2010/801.

15 Accordingly, the names of Mr Koné and Ms Boni-Claverie were, by means of Decision 2011/17, included in the
list in Annex II to Decision 2010/656, as amended by Decision 2010/801.

16 On 14 January 2011 the Council adopted Decision 2011/18 in order to impose additional restrictive measures, in particular the freezing of funds, economic resources belonging to, owned, etc., and in particular who are jeopardising the proper outcome of the electoral process, or held by entities owned or controlled directly or indirectly by them or by any persons acting on their behalf or at their direction, as designated by the Sanctions Committee.

17 Under Article 5(1)(b) and (2) of Decision 2010/656 as amended by Decision 2011/18:‘1. All funds and economic resources owned or controlled directly or indirectly by:
   (a) the persons referred to in Annex I designated by the Sanctions Committee, or held by entities owned or controlled directly or indirectly by them or by any persons acting on their behalf or at their direction, as designated by the Sanctions Committee,
   (b) the persons or entities referred to in Annex II who are not included in the list in Annex I and who are obstructing the process of peace and national reconciliation, and in particular who are jeopardising the proper outcome of the electoral process, or held by entities owned or controlled directly or indirectly by them or by any persons acting on their behalf or at their direction, shall be frozen.
   2. No funds, financial assets or economic resources shall be made available, directly or indirectly, to or for the benefit of persons or entities referred to in paragraph 1.’

18 In order to ensure consistency with the process for amending and reviewing Annexes I and II to Decision 2010/656 as amended by Decision 2011/18, the Council adopted, on 14 January 2011, Regulation No 25/2011.

19 Article 2 of Regulation No 560/2005, as amended by Regulation No 25/2011, states:
   ‘1. All funds and economic resources belonging to, owned, held or controlled by the natural or legal persons, entities and bodies listed in Annex I or in Annex IA shall be frozen.
   2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies listed in Annex I or in Annex IA.
   3. The participation, knowing and intentional, in activities the object or effect of which is, directly or indirectly, to circumvent the measures referred to in paragraphs 1 and 2 shall be prohibited.
   4. Annex I shall consist of the natural or legal persons, entities and bodies referred to in Article 5(1)(a) of Decision 2010/656 as amended.
   5. Annex IA shall consist of the natural or legal persons, entities and bodies referred to in Article 5(1)(b) of Decision 2010/656 as amended.’

20 By means of Decision 2011/18 and Regulation No 25/2011 the Council maintained the names of Mr Gbagbo, Mr Koné, Mr N’Guessan and Ms Boni-Claverie in the list in Annex II to Decision 2010/656, as amended by Decision 2011/17, and also entered their names in the list in Annex IA to Regulation No 560/2005, as amended by Regulation No 25/2011.

21 On 30 March 2011 the United Nations Security Council adopted Resolution 1975 (2011), Annex I to which lists a number of persons who had obstructed peace and reconciliation in Côte d’Ivoire, had obstructed the work of the United Nations Operation in Côte d’Ivoire (UNOCI) and other international actors in Côte d’Ivoire and had committed serious violations of human rights and international humanitarian law. Mr Gbagbo, Mr Djédjé and Mr N’Guessan are named in Annex I.

22 On 6 April 2011 the Council adopted Decision 2011/221 and Regulation No 330/2011 whereby it, inter alia, imposed additional restrictive measures and amended the lists of persons and entities in Annexes I and II to Decision 2010/656, as amended by Decision 2011/18, and in Annexes I and IA to Regulation No 560/2005, as amended by Regulation No 25/2011.

23 Decision 2011/221 in particular removed the names of Mr Gbagbo and Mr N’Guessan from the list in Annex II to Decision 2010/656, as amended by Decision 2011/18, and added their names to the list in Annex I to Decision 2010/656, as amended.

24 Further, Decision 2011/221 added the name of Mr Djédjé to the list in Annex I to Decision 2010/656, as amended by Decision 2011/18.

25 Regulation No 330/2011, for its part, removed the names of Mr Gbagbo and Mr N’Guessan from the list in Annex IA to Regulation No 560/2005, as amended by Regulation No 25/2011, and added their names to the list in Annex I to Regulation No 560/2005, as amended.

26 Regulation No 330/2011 also added the name of Mr Djédjé to the list in Annex I to Regulation No 560/2005, as amended by Regulation No 25/2011.

27 Article 7 of Decision 2010/656, as amended by Decision 2010/801, provides:
   ‘1. Where the Security Council or the Sanctions Committee designates a person or entity, the Council shall include such person or entity in the list in Annex I.
   2. Where the Council decides to apply to a person or entity the measures referred to in Article 4(1)(b), it shall amend Annex II accordingly.
   3. The Council shall communicate its Decision, including the grounds for listing, to the person or entity concerned, either directly, if the address is known, or through the publication of a notice, providing such person or entity with an opportunity to present observations.
   4. Where observations are submitted, or where substantial new evidence is presented, the Council shall review its Decision and inform the person or entity accordingly.’

28 Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011, provides:
   ‘The Council shall communicate its decision, including the grounds for listing, to the person or entity referred to in paragraphs 1 and 2, either directly, if the address is known, or through the publication of a notice, providing such natural or legal person, entity or body with an opportunity to present observations.
   29 The Council published in the Official Journal of the European Union of 18 January 2011 and 7 April 2011 notices for the attention of the persons to whom the restrictive measures laid down in the contested measures applied [OJ 2011 C 14, p. 8, and OJ 2011 C 180, pp. 2 and 4]. In those notices the Council intimates the existence of those restrictive measures, refers to the relevant texts in relation to the reasons for each listing and draws attention to the possibility of making an application to the competent authorities of the relevant Member State in order to obtain authorisation to use frozen funds for basic needs or to make specific payments. The Council further adds that the persons and entities concerned may submit a request for reconsideration. Finally the Council gives notice of the possibility of challenging its decision before the General Court, in accordance with the conditions laid down in the second paragraph of Article 275 TFEU and the fourth and sixth paragraphs of Article 263 TFEU.
   The procedure before the General Court and the orders under appeal
   30 By applications lodged at the Registry of the General Court on 7 July 2011, the appellants sought the annulment of the contested measures in so far as those measures concerned them. In support of their action, they relied on, first, an infringement of the rights of the defence and of the right to an effective remedy and, secondly, an infringement of their rights of property and free movement.
   31 The appellants further claimed that their actions should be declared to be admissible by the General Court, since the time-limit of two months laid down in Article 263 TFEU for the bringing of an action could not apply to them given the failure to notify them of the contested measures.
   32 By the orders under appeal, the General Court dismissed the actions as being manifestly inadmissible.
   33 The General Court first recalled the settled case-law that the time-limit for bringing an action laid down in the
The appellants claim that the Court should:
- set aside the orders under appeal and declare their actions at first instance to be admissible;
- refer the cases back the General Court for it to give a ruling on the substance, and
- order the Council to pay the costs.

40 The Council contends that the Court should:
- dismiss the appeals; and
- order the appellants to pay the costs.

41 By order of the President of the Court of 14 December 2011, Cases C-478/11 P to C-492/11 P were joined for the purposes of the written and oral procedure and the judgment.

42 By letter dated 11 May 2012, sent by fax and registered mail, the Registrar of the Court informed the parties that a hearing would be held on 26 June 2012 and asked them to reply in writing no later than by 15 June 2012 to the questions of the Court annexed to the notification of the hearing.

43 The Council's reply to the question put to it was received at the Registry of the Court on 14 June 2012. However, the time-limit of 15 June 2012 passed without any reply being received by the Court from the appellants to the question put to them or any reply as regards whether they would attend the hearing.

44 A final time-limit was set for the appellants to indicate whether they would attend the hearing. That time-limit of 21 June 2012 having passed without reply from them, the hearing was cancelled.

The appeals

45 In support of their appeals, the appellants rely on two grounds. By the first ground of appeal, they claim that the General Court erred in law by not accepting the existence of unforeseeable circumstances or of force majeure. By the second ground of appeal, the appellants claim that the General Court was wrong to hold that the time-limit for bringing proceedings and the principle of legal certainty underlying that time-limit barred their action where the distinguishing features of this case were, first, that there was no notification of the contested measures and, secondly, the inapplicability of the extension of the time-limit on account of distance as set out in the Rules of Procedure of the General Court.

46 The second ground of appeal should be examined first.

The second ground of appeal

Arguments of the parties

47 The appellants claim, first, that the General Court disregarded the principle of effective judicial protection and thus erred in law by holding that, since the contested measures had been published, the time-limit for bringing proceedings should be calculated from the date of their publication. According to the appellants, the General Court ought to have taken account of the fact that the contested measures had not, contrary to the provisions of, in particular, Article 7(2) of Decision 2010/656, as amended by Decision 2010/801, been notified, as there had been no individual communication to put the persons affected by the measures in a position to take cognisance of them.

48 The appellants consider, secondly, that the General Court should not have applied the provisions of Article 102(2) of its Rules of Procedure on the extension of the time-limit on account of distance to the appellants, residing in a State in Africa, particularly when that State was in a situation of armed conflict.

49 The Council contends that the procedural context of the present cases is not the same as that examined by the Court in its judgment of 16 November 2011 in Case C-548/09 P Bank Melli Iran v Council [2011] ECR I-11381. In that judgment, the Court based the obligation to communicate individually the reasons for the adoption of restrictive measures on Article 15(3) of Council Regulation (EC) No 423/2007 of 19 April 2007 concerning restrictive measures against Iran (OJ 2007 L 153, p. 1). Unlike Regulation No
423/2007, Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, provides for the possibility of communication through the publication of a notice in cases where the address of the person concerned is not known to the Council.

50 In this case, the Council contends that it communicated the contested measures to the appellants by means of a published notice, in accordance with Article 7(3) of Decision 2010/656, as amended by Decision 2010/801. The Council argues that it could not have communicated the measures otherwise, since the private addresses of the appellants were not known.

51 In any event, according to the Council, the date of publication of the contested measures marked the starting point for the calculation of the period established in Article 263 TFEU. That interpretation follows from the requirements of legal certainty which permeate the rules on procedural time-limits.

52 Lastly, the Council states that the appellants’ arguments on the extension of the time-limit on account of distance are manifestly unfounded and amount, in essence, to a challenge to the validity of Article 102(2) of the General Court’s Rules of Procedure. That provision is however no more than an extension of the period laid down in the sixth paragraph of Article 263 TFEU.

Findings of the Court

53 First, it must be stated that the General Court was correct to hold that it is entitled to examine of its own motion whether the time-limit for bringing proceedings has been observed, that being a matter of public policy (see, inter alia, Case 79/70 Müller v CES [1971] ECR 689, paragraph 6, and Transports Evaristo Molina v Commission, paragraph 33).

54 It must next be recalled that, according to the sixth paragraph of Article 263 TFEU, ‘proceedings provided for in this article shall be instituted within two months of the publication of the measure, or of its notification to the plaintiff, or, in the absence thereof, of the day on which it came to the knowledge of the latter, as the case may be’.

55 In this case, the contested measures were published in the Official Journal of the European Union, Series L, but were also, pursuant to Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, and Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011, to be communicated to the persons and entities concerned, either directly if their addresses were known, or, if not, through the publication of a notice.

56 That situation is a consequence of the particular nature of the contested measures, which at the same time resemble both measures of general application on a category of addressees determined in a general and abstract manner a prohibition on, inter alia, making available funds and economic resources to persons and entities named in the lists contained in their annexes and also a bundle of individual decisions affecting those persons and entities (see, to that effect, Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission [2008] ECR I-6351, paragraphs 241 to 244).

57 It must, moreover, be recalled that, as regards measures adopted on the basis of provisions relating to the Common Foreign and Security Policy, such as the contested measures, it is the individual nature of those measures which, in accordance with the second paragraph of Article 275 TFEU and the fourth paragraph of Article 263 TFEU, permits access to the Courts of the European Union.

58 Having regard to those particular features and the consequent rules relating to publication and communication, the sixth paragraph of Article 263 TFEU would not be applied consistently if, when applied to persons and entities who are named in the lists contained in the annexes to those measures, the starting point for the calculation of the period for bringing an action for annulment was, for those persons, fixed as the date of publication of the measure at issue and not as the date when that measure was communicated to them. The purpose of that communication is precisely to ensure that persons to whom the measures are addressed are able to defend their rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in bringing proceedings to the Courts of the European Union (Kadi and Al Barakaat International Foundation v Council and Commission, paragraph 337).

59 It follows that while, admittedly, the entry into force of measures such as the contested measures is effected by their publication, the period for the bringing of an action for the annulment of those measures under the fourth paragraph of Article 263 TFEU runs, for each of those persons and entities, from the date of the communication which they must receive.

60 In the present case, contrary to what is claimed by the appellants, the contested measures were communicated to them.

61 It is true that those measures were not directly communicated to them at their addresses. As the Council found that it was impossible to undertake direct communication to Mr Gbagbo, Mr Koné, Ms Boni-Claireville, Mr Djédjé and Mr N’Guessan, it had recourse to publication of the notice provided for in Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, and in Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011. The Council therefore published, in the Official Journal of the European Union, Series C, of 18 January 2011 and 7 April 2011, the notices referred to in paragraph 29 of this judgment.

62 Given that such notices are capable of enabling the persons concerned to identify the legal remedies available to them in order to challenge their designation in the lists concerned and the date when the period for bringing proceedings expires (Case C-417/11 P Council v Bamba [2012] ECR, paragraph 81), it is important that the appellants should not be able to defer the starting point of the period for bringing proceedings by relying on the fact that there was no direct communication or that they actually became aware of the contested measures at a later date. If such a possibility were, in the absence of force majeure, open to the appellants, it would jeopardise the very objective of a time-limit for bringing proceedings, which is to protect legal certainty by ensuring that European Union measures which produce legal effects may not indefinitely be called into question (see, inter alia, Case C-179/95 Wilic [1997] ECR I-585, paragraph 19; Case C-241/01 National Farmers’ Union [2002] ECR I-9079, paragraph 34, and order of 15 November 2012 in Case C-102/12 P Städtler v ECR, paragraph 12).

63 As regards, lastly, the appellants’ argument that the extension of the time-limit on account of distance by ten days as provided for in paragraph 102(2) of the General Court’s Rules of Procedure cannot be applied to them because they are established in a non-Member State, suffice it to observe that that argument is invalidated by the fact that the extension is for a single fixed period. It follows that the fact that the appellants were, during the period for bringing proceedings, in a non-Member State, does not, in itself, mean that they were in a situation which was objectively different, with regard to the application of that time-limit, from the situation of persons and entities established within the European Union who were the subject of restrictive measures of the same nature as the contested measures.

64 It follows from all the foregoing that, even though the General Court erred in law by holding that the periods for bringing proceedings started to run on the dates of publication of the contested measures, those periods, which should have been calculated from the dates referred to in paragraph 61 of this judgment, had expired on 7 July 2011, the date when the actions were brought. That being the case, the second ground of appeal must be rejected (see, by analogy, Case C-282/05 P Holcim (Deutschland) v Commission [2007] ECR I-2941, paragraph 33).

The first ground of appeal
Arguments of the parties
65 The appellants submit that the General Court infringed Article 45 of the Statute of the Court of Justice by not finding that there was force majeure for the purposes of that article.
66 The appellants claim that the armed conflict which took place in Côte d'Ivoire should be regarded as a case of force majeure as far as they are concerned, since, during that period, they had no means of communication whereby they could become aware of the contested measures and therefore could not exercise their right to bring proceedings.
67 The Court states that one of the constituent elements of the concept of force majeure is the occurrence of an event outside the control of the person who wishes to rely on it, that is to say when something happens which the person concerned can take no action to influence (Case C-334/08 Commission v Italy [2010] ECR I-6869, paragraph 47). Yet the post-election crisis in Côte d'Ivoire and the violence associated with that crisis were provoked by the refusal of Mr Gbagbo and his colleagues to surrender power to the elected President. Those circumstances are therefore not outside the control of the appellants.

Findings of the Court
68 Under the second paragraph of Article 45 of the Statute of the Court, ‘no right shall be prejudiced in consequence of the expiry of a time-limit if the party concerned proves the existence of unforeseeable circumstances or of force majeure.’
69 It is clear that, as stated by the General Court in the orders under appeal, the appellants did not argue before it that such circumstances existed.
70 The Court has however held that an appellant cannot be criticised for relying for the first time at the appeal stage on the existence of force majeure where the General Court gave its decision by order on the basis of Article 111 of its Rules of Procedure, did not inform the applicant of its intention to dismiss his action as being out of time and did not ask the applicant to explain the delay in the arrival of the Registry of the original of the application (order of 18 January 2005 in Case C-325/03 P Zuazaga Meabe v OHIM [2005] ECR I-403, paragraph 24). The appellants’ first ground of appeal on the existence of force majeure must therefore be examined.
71 In that regard, it must first be recalled that the strict application of procedural rules serves the requirements of legal certainty and the need to avoid any discrimination or arbitrary treatment in the administration of justice (Case C-426/10 P Bell & Ross v OHIM [2011] ECR I-8849, paragraph 43 and case-law cited).
72 It must next be observed that, in accordance with the sixth paragraph of Article 263 TFEU and Article 45 of the Statute of the Court, it is for the party concerned to establish, first, that abnormal circumstances, unforeseeable and outside his control, made it impossible for him to comply with the time-limit for bringing proceedings laid down in the sixth paragraph of Article 263 TFEU and, secondly, that he could not guard against the consequences of those circumstances by taking appropriate steps without making unreasonable sacrifices (see, to that effect, Case C-314/06 Société Pipeline Méditerranée et Rhône [2007] ECR I-12273, paragraph 24 and case-law cited).
73 In this case, the appellants make general reference to there being in Côte d’Ivoire a situation of armed conflict, which according to them began in November 2010 and continued at least until April 2011.
74 However, none of the appellants has presented, in their appeals before the Court, any material which might enable the Court to understand in what way and for what specific period of time the general situation of armed conflict in Côte d’Ivoire and the personal circumstances relied on by the appellants prevented them from bringing their actions in good time.
75 In those circumstances, the first ground of appeal must be rejected.
76 Since neither of the grounds relied on by the appellants is well founded, the appeals must be dismissed.

Costs
77 Under Article 138(1) of the Court’s Rules of Procedure, which applies to the procedure on appeal by virtue of Article 184(1) thereof, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party’s pleadings. Since the Council has applied for costs and the appellants have been unsuccessful, the appellants must be ordered to pay the costs.

On those grounds, the Court (Grand Chamber) hereby
1. Dismisses the appeals;
2. Orders Mr Laurent Gbagbo, Mr Katinan Justin Koné, Ms Akissi Daniele Boni-Claevers, Mr Alcide Djedje and Mr Affi Pascal Ngueassan to pay the costs.

[Signatures]

C-212/11, Jyske Bank Gibraltar Ltd v Administración del Estado

JUDGMENT OF THE COURT (Third Chamber)
25 April 2013 (*)

In Case C-212/11,
REQUEST for a preliminary ruling under Article 267 TFEU from the Tribunal Supremo (Spain), made by decision of 21 March 2011, received at the Court on 9 May 2011, in the proceedings Jyske Bank Gibraltar Ltd

Administración del Estado,

2 The request has been made in proceedings between Jyske Bank Gibraltar Ltd [‘Jyske’], a credit institution situated in Gibraltar operating in Spain under the rules on the freedom to provide services, and the Administración del Estado concerning the decision of the Consejo de Ministros (Spanish Council of Ministers) of 23 October 2009 which rejected the application for review brought against the decision of that Consejo de Ministros of 17 April 2009 imposing on Jyske two financial penalties for a total amount of EUR 1 700 000 and two public reprimands following a refusal or lack of diligence to provide the information requested by the Servicio Ejecutivo de la Comisión para la Prevención de Blanqueo de Capitales (Executive service for the prevention of money laundering) (‘the Servicio Ejecutivo’).

Legal context
European Union law
‘(1) Member States shall ensure that the institutions and persons subject to this Directive and their directors and employees cooperate fully with the authorities responsible for combating money laundering:
(a) by informing those authorities, on their own initiative, of any fact which might be an indication of money laundering;
(b) by furnishing those authorities, at their request, with all necessary information, in accordance with the procedures established by the applicable legislation.

(2) The information referred to in paragraph 1 shall be forwarded to the authorities responsible for combating money laundering of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated by the institutions and persons in accordance with the procedures provided for in Article 11(1)(a) shall normally forward the information.

4 Directive 91/308 was repealed and replaced by Directive 2005/60, recital 40 in the preamble to which is worded as follows: ‘Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between financial intelligence units (‘FIUs’), as referred to in Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [(OJ 2000 L 271, p. 4)], including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent. To that end, the Commission should lend such assistance as may be needed to facilitate such coordination, including financial assistance.’

5 Under Article 5 of that directive, ‘[t]he Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.’

6 Article 7 of that directive provides: ‘The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.’

7 Under Article 21 of that directive: ‘(1) Each Member State shall establish an FIU in order effectively to combat money laundering and terrorist financing.

(2) That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.

(3) Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.’

8 Article 22 of Directive 2005/60 provides:

‘(1) Member States shall require the institutions and persons covered by this Directive, and where applicable their directors and employees, to cooperate fully:

(a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted;

(b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

(2) The information referred to in paragraph 1 shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 34 shall normally forward the information.’

9 As is apparent from Article 3(1) and (2)(f) of Directive 2005/60, the institutions referred to in Article 22 thereof also include branches of the institutions referred to in Article 13 of Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions [(OJ 2000 L 126, p. 1)]. A branch is defined in the latter provision as a place of business which forms a legally dependent part of a credit institution and which carries out directly all or some of the transactions inherent in the business of credit institutions.

10 Article 1 of Decision 2000/642 provides:

‘(1) Member States shall ensure that FIUs, set up or designated to receive disclosures of financial information for the purpose of combating money laundering shall cooperate to assemble, analyse and investigate relevant information within the FIU on any fact which might be an indication of money laundering in accordance with their national powers.

(2) For the purposes of paragraph 1, Member States shall ensure that FIUs exchange, spontaneously or on request and either in accordance with this Decision or in accordance with existing or future memoranda of understanding, any available information that may be relevant to the processing or analysis of information or to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved.

(3) Where a Member State has designated a police authority as its FIU, it may supply information held by that FIU to be exchanged pursuant to this Decision to an authority of the receiving Member State designated for that purpose and being competent in the areas mentioned in paragraph 1.’

11 Under Article 4 of that decision:

‘(1) Each request made under this Decision shall be accompanied by a brief statement of the relevant facts known to the requesting FIU. The FIU shall specify in the request how the information sought will be used.

(2) When a request is made in accordance with this Decision, the requested FIU shall provide all relevant information, including available financial information and requested law enforcement data, sought in the request, without the need for a formal letter of request under applicable conventions or agreements between Member States.

(3) An FIU may refuse to divulge information which could lead to impairment of a criminal investigation being conducted in the requested Member State or, in exceptional circumstances, where divulgence of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State concerned or would otherwise not be in accordance with fundamental principles of national law. Any such refusal shall be appropriately explained to the FIU requesting the information.’

12 Article 10 of that decision states that it shall apply to Gibraltar and that, to that effect, notwithstanding Article 2 thereof, the United Kingdom of Great Britain and Northern Ireland may notify to the General Secretariat of the Council of the European Union an FIU in Gibraltar.

National law


14 According to the second paragraph of Article 2 (1) of Law 19/1993: ‘The following shall be subject to the obligations laid down in this law:

(a) Credit institutions

Foreign persons or institutions conducting activities in Spain of the same type as those conducted by the aforementioned
persons or institutions, whether through branches or by providing services without a permanent establishment. The persons in question shall also be subject to the requirements laid down in this law for operations carried out through agents or other legal or natural persons acting as their intermediary.

15 With regard to the information requirements, Article 3 of Law 19/1993 provided as follows: The persons referred to in the above article are subject to the following requirements:

(4) To cooperate with [the Servicio Ejecutivo] and, to that end:

(a) to notify it, on their own initiative, of any fact or transaction which is, or which shows indications of being, connected with the laundering of money deriving from the activities listed in Article 1. The notification shall normally be effected by the person or persons designated by the persons or institutions subject to the obligations hereunder in accordance with the procedures referred to in paragraph 7 of this Article. That person or those persons shall appear in all legal or administrative proceedings of whatever type concerning the information contained in the notification or any other supplementary information which may relate to it. Specific circumstances or transactions of which [the Servicio Ejecutivo] must always be notified shall be defined by regulation.

Transactions which are obviously inconsistent with the nature of activity or previous dealings of customers shall also be notified, provided that no financial, professional or business reason for such transactions emerges from the special examination referred to in paragraph 2, in relation to the activities listed in Article 1 of this law.

16 Article 16(3) of that law provided:

‘In accordance with the guidelines established by the Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, [the Servicio Ejecutivo] and, where appropriate, the Secretaria de esa comisión [that commission] shall cooperate with the authorities performing a similar function in other States, seeking to obtain, in particular, the cooperation of the authorities of those States whose sovereignty extends to territory neighbouring that of [the Kingdom of] Spain …

17 Law 19/1993 was repealed by law 10/2010 on the prevention of money laundering and the financing of terrorism (Ley de prevención del blanqueo de capitales y de la financiación del terrorismo) of 28 April 2010 (BOE No 103 of 29 April 2010, p. 37458), the purpose of which was to transpose Directive 2005/60 into Spanish law. Pursuant to Article 5 of that law, the Servicio Ejecutivo must always be notified shall be defined by regulation.

Transactions which are obviously inconsistent with the nature of activity or previous dealings of customers shall also be notified, provided that no financial, professional or business reason for such transactions emerges from the special examination referred to in paragraph 2, in relation to the activities listed in Article 1 of this law.

18 Article 5(2)(c) of Royal Decree 925/1995, approving the regulation implementing Law 19/1993, of 28 December 1993, on specific measures for preventing money laundering (Real Decreto 925/1995 por el que se aprueba el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales), of 9 June 1995 (BOE No 160, of 6 July 1995, p. 20521), requires that the Servicio Ejecutivo be informed of account transfers to or from tax havens.

19 Article 7(2)(b) of that royal decree provides as follows: ‘Persons or institutions subject to the obligations hereunder shall, in any event, notify the Servicio Ejecutivo on a monthly basis of:

(b) transactions with or by natural or legal persons who are resident in territories or countries which are designated for such purposes by order of the Ministro de Economía y Hacienda, or who are acting on behalf of such resident persons, and transactions involving transfers of funds to or from such territories or countries, regardless of the residence of the parties, provided that the value of such operations is in excess of EUR 30 000 or its equivalent in foreign currency.’

20 Territories regarded as tax havens and uncooperative territories were previously specified by Royal Decree 1080/1991 of 5 July 1991 (BOE No 167, of 13 July 1991, p. 233371) and by order ECO/2652/2002 of 24 October 2002 on the implementation of disclosure obligations in relation to operations with certain States to the Servicio Ejecutivo of the Commission for the prevention of money laundering and monetary offences (Orden ECO/2652/2002 por la que se desarrollan las obligaciones de comunicación de operaciones en relación con determinados países al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias) (BOE No 260 of 30 October 2002, p. 38033). Gibraltar appears on this list.

21 According to the Tribunal Supremo, Article 5 of the Crime (Money Laundering and Proceeds) Act 2007, which transposes directive 2005/60, requires adherence to banking confidentiality.

The dispute in the main proceedings and the question submitted for a preliminary ruling

22 Jyske, a branch of the Danish bank NS Jyske Bank, is a credit institution established in Gibraltar, where it comes under the supervision of the Financial Services Commission.

23 According to the order for reference, Jyske operated, at the time of the facts in the main proceedings, in Spain under the rules on the freedom to provide services, that is to say, without being established there.

24 On 30 January 2007, the Spanish FIU, namely the Servicio Ejecutivo, informed Jyske that if it did not designate an agent authorised to deal with it, the Servicio Ejecutivo would have to investigate the structure of Jyske’s organisation and procedures with regard to activities carried out by it in Spain under the freedom to provide services. At this time, the Servicio Ejecutivo asked Jyske to provide, by 1 March 2007, documents and information relating, in particular, to the identity of its customers.

25 That request was made following a report of the Servicio Ejecutivo of 24 January 2007, which stated that Jyske was carrying on in Spain a substantial operation comprising, inter alia, the grant of mortgages for the purchase of property in Spain. The report stated that ‘in order to develop such an operation in Spain, the institution has dual support or backing, namely from the branch in Spain of the parent company and from two firms of lawyers in Marbella (Spain). According to information in the public domain, the property investor undertakes for one of the two firms to be investigated for money laundering offences and his name appears, as does the name of the other firm of lawyers mentioned above, in connection with a number of operations divulged to the Servicio Ejecutivo by other persons subject to a duty of disclosure regarding evidence of money laundering.’ In the light of those facts, the Servicio Ejecutivo considered that there was a very high risk that Jyske was being used for money laundering operations in the context of its activities in Spain under the freedom to provide services. According to the report of the Servicio Ejecutivo of 24 January 2007, the mechanism used for this purpose consisted in creating in Gibraltar ‘corporate structures ultimately intended to prevent detection of the identity of the actual and final owner of property acquired in Spain, essentially on the Costa del Sol and of … the origin of the monies used for the purposes of such acquisition.

26 On 23 February 2007, Jyske sent a communication to the Servicio Ejecutivo informing it that it had applied to its supervisory authority, the Financial Services Commission, for an opinion to establish whether it was entitled to provide such information without infringing Gibraltar legislation on banking confidentiality and the protection of personal data. On 14 March 2007, that commission requested the Servicio
Ejecutivo to enter into a process of mutual cooperation. By letter of 2 April 2007, the Servicio Ejecutivo informed that commission that Jyske was subject to obligations in relation to its activities in Spain.

Consequently, on 25 October 2007, the general secretariat of the Servicio Ejecutivo opened an investigation into Jyske, accusing it, in particular, of having infringed the provisions of Law 19/1993, committed a very serious offence, defined as follows: [the] refusal or lack of diligence to supply precise information requested in writing by the Servicio Ejecutivo and [the] failure to comply with its obligation to supply information relating to specific cases established by way of a regulation (systematic reports). Consequently it made an order against Jyske for two public reprimands and two financial penalties for a total amount of EUR 1 700 000.

On 30 April 2009, Jyske brought an appeal against that decision before the Consejo de Ministros, which was dismissed by the latter on 23 October 2009. Jyske then brought an administrative appeal before the Tribunal Supremo. Jyske claims, in support of that appeal, to fulfil its disclosure obligations under Law 19/1993, committed a very serious offence, defined as follows: [the] refusal or lack of diligence to supply precise information requested in writing by the Servicio Ejecutivo and [the] failure to comply with its obligation to supply information relating to specific cases established by way of a regulation (systematic reports). Consequently it made an order against Jyske for two public reprimands and two financial penalties for a total amount of EUR 1 700 000.

On 30 April 2009, Jyske brought an appeal against that decision before the Consejo de Ministros, which was dismissed by the latter on 23 October 2009. Jyske then brought an administrative appeal before the Tribunal Supremo. Jyske claims, in support of that appeal, that, under Directive 2005/60, it is only subject to an obligation of disclosure vis-à-vis the Gibraltar authorities, and that, in so far as the Spanish legislation extends that obligation to credit institutions operating in Spain under the freedom to provide services, it does not comply with the provisions of that directive.

It is in those circumstances that the Tribunal Supremo decided to stay the proceedings and to refer the following question to the Court for a preliminary ruling: 'Does Article 22(2) of Directive 2005/60/EC ... permit a Member State to make it a mandatory requirement that the information which must be provided by credit institutions operating in its territory without a permanent establishment be forwarded directly to its own authorities responsible for the prevention of money laundering, or, on the other hand, must the request for information be directed to the [FIU] of the Member State in whose territory the addressee institution is situated?'

The question referred for a preliminary ruling: Admissibility

The Kingdom of Spain considers that the question referred is inadmissible because it is purely hypothetical and has no connection with the subject-matter of the main proceedings, to the extent that it concerns the interpretation of Article 22(2) of Directive 2005/60, which should have been transposed by 15 December 2007 at the latest, although the request for information sent to Jyske took effect between 30 January and 12 June 2007.

In that regard, it must be borne in mind that, according to settled case-law, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted concern the interpretation of European Union law, the Court is in principle required to give a ruling (Case C-416/10 Krftan and Others [2013] ECR, paragraph 53 and the case-law cited).

It follows that questions concerning European Union law enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of European Union law that is sought is unrelated to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (Joined Cases C-570/07 and C-571/07 Blanco Pérez and Chao Gómez [2010] ECR I-4629, paragraph 36; and Case C-509/10 Gießbeck [2012] ECR, paragraph 48).

Directive 2005/60, interpretation of which is requested, entered into force on 15 December 2005, that is to say, before the requests for information sent by the Servicio Ejecutivo to Jyske on 30 January and 12 June 2007. Moreover, although, admittedly, the period allowed for transposition of that directive expired only on 15 December 2007, the main proceedings concern nevertheless the lawfulness of the decision adopted against Jyske by the Consejo de Ministros on 23 October 2009, that is to say, after the expiry of that period for transposition.

It follows that the request for a preliminary ruling is admissible.

Substance

By its question, the referring court asks, in essence, whether Article 22(2) of Directive 2005/60 must be interpreted as precluding a Member State's national legislation which requires credit institutions carrying on their activities under the freedom to provide services in that Member State to communicate information required for the purpose of combating money laundering directly to the FIU of that Member State.

It should be noted, first of all, that, according to established case-law, in order to provide a satisfactory answer to the national court which has referred a question to it, the Court of Justice may deem it necessary to consider provisions of European Union law to which the national court has not referred in its question (Case C-230/06 Millitzer & Münch [2008] ECR I-1895, paragraph 19).

In the present case, the answer to the question submitted does not depend solely on the interpretation of Article 22(2) of Directive 2005/60, but requires that account be taken, also, first of all, of the provisions of that directive, and of Decision 2000/642, and, secondly, of Article 56 TFEU.

Directive 2005/60

Concerning Article 22(2) of Directive 2005/60, it is expressly apparent from the wording thereof that the institutions and persons subject to the requirements arising from the latter must forward information necessary to prevent money laundering and terrorist financing to the FIU of the Member State in whose territory they are situated.

Contra to what the Spanish Government claims, the wording 'the Member State in whose territory the institution or person forwarding the information is situated', cannot be interpreted as referring, in the case of an activity carried out by the entity concerned under the rules on the freedom to provide services, to the territory of the host Member State where the activity is performed.

First, that reading does not correspond to the ordinary meaning of the words in question. Secondly, Article 22(2) of that directive does not make a distinction between services provided in the Member State where the entity is situated and those performed in other Member States under the rules on the freedom to provide services, nor, a fortiori, does it state, with regard to the services provided under the rules on the freedom to provide services, that the competent FIU must be that of the Member State in which those services are provided.

It follows that Article 22(2) of that directive must be interpreted as meaning that the entities referred must forward the requested information to the FIU of the Member
State in whose territory they are situated, that is to say, in the case of operations performed under the rules on the freedom to provide services, to the FIU of the Member State of origin.

44 It is, however, necessary to consider whether that provision alone is not the less precludes the host Member State from requiring a credit institution carrying out activities in its territory under the rules on the freedom to provide services to forward the information referred directly to its own FIU.

45 It should be noted in that regard, first, that the wording of Article 22(2) of Directive 2005/60 does not expressly prohibit such a possibility.

46 Secondly, it should be pointed out that whilst, admittedly, Directive 2005/60 was founded on a dual legal basis (namely, Article 47(2) EC [now Article 53(1) TFEU], and Article 95 EC [now Article 114 TFEU]), it seeks therefore also to ensure the proper functioning of the internal market, its main aim, is the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, as is apparent both from its title and the preamble, and from the fact that it was adopted, like its predecessor, Directive 91/308, in an international context, in order to apply and make binding in the European Union the recommendations of the 'Financial Action Task Force' (FATF), which is the main international body combating money laundering.

47 Consequently, legislation, such as that at issue in the main proceedings, which seeks to allow the competent authorities of the host Member State to obtain information necessary to more effectively combat money laundering and terrorist financing, paves the way to an aim similar to that of Directive 2005/60.

48 Third, Directive 2005/60 does not deprive the authorities of the Member State where suspicious operations or transactions are carried out of their competence to investigate and pursue cases of money laundering. Such is the case where operations are carried out by means of the freedom to provide services.

49 It follows that Article 22(2) of Directive 2005/60 does not, in principle, preclude Member State legislation which requires credit institutions carrying out activities in its territory under the rules on the freedom to provide services to forward the required information directly to its own FIU, in so far as such legislation seeks to strengthen, in compliance with European Union law, the effectiveness of the fight against money laundering and terrorist financing.

50 Therefore, such legislation cannot compromise the principles established by Directive 2005/60 concerning the reporting requirements on the part of entities subject to them, nor can it impair the effectiveness of existing forms of cooperation and exchange of information between the FIUs, as provided for by Decision 2000/642.

51 In that regard, it should be noted, first, that the adoption by a Member State of legislation requiring financial institutions situated in another Member State and operating under the freedom to provide services in its territory to forward directly to their own FIU information necessary to combat money laundering and terrorist financing cannot relieve credit institutions covered by Directive 2005/60 of their obligation to supply the required information to the FIU of the Member State in whose territory they are situated, in compliance with Article 22 of that directive.

52 Concerning, secondly, coordination and cooperation between the FIUs, as provided for by Directive 2005/60 and Decision 2000/642, it is apparent from recital 40 in the preamble to that directive that 'Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between FIUs as referred to in ... Decision 2000/642 ..., including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent'.

53 In that regard, it should be noted, first of all, that whilst Directive 2005/60 lays down numerous concrete and detailed requirements on customer due diligence, on disclosure and keeping of records, which the Member States must impose on the financial institutions covered, it does not, concerning cooperation between the FIUs, itself lay down any requirements or procedures, but merely states, in Article 58, that the 'Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community'.

54 It must be noted, next, that national legislation, such as that at issue in the main proceedings, does not infringe any provisions of Decision 2000/642 where the FIU of the Member State which adopted such legislation is in no way exempted from its requirement to cooperate with the FIUs of other Member States and, reciprocally, retains, unchanged, the right to require them to forward documents or information for the purpose of combating money laundering.

55 Such legislation does not undermine the mechanism for cooperation between the FIUs provided for by Decision 2000/642, but envisages, outside the context of the latter, a means for the FIU of the Member State concerned to obtain directly information in the specific case of an activity carried out under the freedom to provide services in its territory.

56 It follows from the foregoing that Article 22(2) of Directive 2005/60 does not preclude national legislation, such as that at issue in the main proceedings, where it complies with the conditions set out in paragraphs 49 to 51 and 54 of this judgment.

Article 56 TFEU

57 In order to determine whether European Union law has been complied with for the purposes of paragraph 49 of this judgment, it is necessary again to consider whether Article 56 TFEU precludes national legislation, such as that at issue in the main proceedings, according to which a credit institution which provides services in the territory of the Member State concerned without being established there is required to forward directly to the FIU of that host Member State its reports on suspicious operations and information that that authority requests from it.

58 It is settled case-law of the Court of Justice that Article 56 TFEU requires not only the elimination of all discrimination against providers of services on grounds of nationality or the fact that they are established in a Member State other than that where the services are to be provided, but also the abolition of any restriction, even if it applies without distinction to national providers of services and to those of other Member States, which is liable to prohibit, impede or render less advantageous the availability of a provider of services established in another Member State where such services go beyond similar services (Joined Cases C-369/96 and C-376/96 Arblade and Others [1999] ECR I-8453, paragraph 33, and Case C-577/10 Commission v Belgium [2012] ECR, paragraph 38 and the case-law cited).

59 Legislation of one Member State, such as that at issue in the main proceedings, which requires credit institutions operating in the territory of that Member State under the freedom to provide services from the territory of another Member State to provide information directly to the FIU of the first Member State, constitutes a restriction on the freedom to provide services, in so far as it gives rise to difficulties and additional costs for activities carried out under the rules governing the freedom to provide services and is liable to be additional to the controls already conducted in the Member State where the institution at issue is situated, thus dissipating the latter from carrying on such activities.

60 Nevertheless, according to the Court's established case-law, where national legislation falling within an area which has not been completely harmonised at European Union level is applicable without distinction to all persons and undertakings operating in the territory of the Member State concerned, it may, notwithstanding its restrictive effect on the freedom to provide services, be justified where it meets
an overriding requirement relating to the public interest and that interest is not already safeguarded by the rules to which the service provider is subject in the Member State in which he is established and in so far as it is appropriate for securing the attainment of the aim which it pursues and does not go beyond what is necessary in order to attain it (see Arblade and Others, paragraphs 34 and 35, and Case C-168/04 Commission v Austria [2006] ECR I-9041, paragraph 37).

61 The combating of money laundering has not been completely harmonised at European Union level. Directive 2005/60 provides for a minimum level of harmonisation and, in particular, Article 5 thereof allows Member States to adopt stricter provisions, where those provisions seek to strengthen the combating of money laundering or terrorist financing.

- Overriding reasons in the public interest

62 The prevention of and the combating of money laundering and terrorist financing are legitimate aims which the Member States have endorsed both at the international and European Union levels.

63 As is stated in the first recital in the preamble to Directive 2005/60, which seeks to implement at European Union level the Recommendations of the FATF, '[m]assive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society'. Likewise, the second recital in the preamble notes that '[i]n order to facilitate their criminal activities, money launderers and terrorist financiers could try to take advantage of the freedom of capital movements and the freedom to supply financial services'.

64 The Court has moreover already accepted that the combating of money laundering, which is related to the aim of protecting public order, constitutes a legitimate aim capable of justifying a barrier to the freedom to provide services (see, to that effect, Case C-212/08 Zeturf [2011] ECR I-5633, paragraphs 45 and 46).

- Suitability of the national legislation at issue for attaining the aims it pursues

65 Since the host Member State authorities have exclusive jurisdiction with regard to the criminalisation, detection and eradication of offences, such as money laundering and terrorism, committed on its territory, it is justified that information concerning suspicious transactions carried out on the territory of that Member State be forwarded to the FIU thereof. National legislation, such as that at issue in the main proceedings, enables the Member State concerned to require, any time where there is reasonable doubt as to the legality of a financial transaction, information which it deems necessary for the national authorities to accomplish their duty and, where appropriate, to pursue and punish those responsible.

66 Furthermore, as the Advocate General has pointed out in point 109 of his Opinion, such legislation enables the Member State concerned to supervise all financial transactions carried out by credit institutions in its territory, and whatever the manner in which those institutions have chosen to provide their services, whether by establishing a registered office or branch, or under the freedom to provide services. In this way, in accordance with the Court's established case-law, which states that national legislation is appropriate for ensuring attainment of the aim pursued only if it genuinely reflects a concern to attain it in a consistent and systematic manner (Case C-169/07 Hartlauer [2009] ECR I-1721, paragraph 55), all the operators are subject to similar obligations, since they are carrying out their activities in the same national territory and offering similar financial services which may, to a greater or lesser degree, be used for the purposes of money laundering or terrorist financing.

67 Consequently, national legislation, such as that at issue in the main proceedings, which requires that information be forwarded to the host Member State FIU concerning activities carried on under the freedom to provide services on the territory of that Member State appears to be suitable so as to attain, effectively and coherently, the aim pursued by that national legislation.

- Proportionality

68 According to established case-law, measures which restrict the freedom to provide services may be justified by the aim which they pursue only if they are suitable for securing the attainment of that aim and do not go beyond what is necessary in order to attain it (see, to that effect, Case C-255/04 Commission v France [2006] ECR I-5251, paragraph 44 and the case-law cited).

69 In order to effectively combat money laundering and terrorist financing, a Member State must be able to obtain the information necessary to enable it to identify and pursue possible infringements in that regard which take place in its territory or which involve persons established on that territory.

70 National legislation, such as that at issue in the main proceedings, which requires credit institutions operating under the freedom to provide services in its territory to provide that information directly to their own FIU will however be proportionate only where the mechanism provided for in Article 22(2) of Directive 2005/60, together with Decision 2000/642, does not already allow that FIU to obtain that information through the FIU of the Member State where the credit institution is situated and to combat money laundering and terrorist financing just as effectively.

71 The receipt, by the FIU of the host Member State, of necessary information from the FIU of the Member State of origin involves, for the credit institution concerned, a lower administrative and financial burden than the requirement to provide that information directly to the FIU of the host Member State. First, it is possible that the FIU of the Member State of origin already has the information requested since the credit institution is required to forward the information to it in accordance with Article 22(2) of Directive 2005/60.

72 Secondly, where the FIU of the Member State in which the credit institution is situated in turn requests that information from the said institution, the administrative burden would also be lower, to the extent that the credit institution would be required to answer to only one interlocutor.

73 In that regard, it must be noted that that mechanism for cooperation between FIUs suffers from certain deficiencies.

74 First of all, it should be pointed out that Decision 2000/642 provides for important exceptions to the requirement for the requested FIU to forward the information requested to the applicant FIU. Thus, Article 4(3) of that decision provides that an FIU may refuse to divulge information which could hinder a judicial inquiry carried out in the Member State of which requisition is made or where divulging information would have consequences which are clearly disproportionate in the light of the legitimate interests of a natural or legal person or the Member State concerned, or also where divulging such information would result in an infringement of the fundamental principles of national law, without, however, defining those concepts.

75 Likewise, it is not disputed that, when combating money laundering or terrorist financing, and, a fortiori, preventing those activities, authorities must act as quickly as possible. Article 22(1) of Directive 2005/60 states expressly that the information referred to must be provided promptly by the credit institutions, whether it concerns spontaneous
disclosure of suspicious operations or necessary information requested by the competent FIU. Consequently, the forwarding of necessary information directly to the FIU of the Member State in whose territory the operations were carried out appears to be the most appropriate means of ensuring effective combating of money laundering or terrorist financing.

76. Next, Decision 2000/642 does not lay down a time-limit for information to be forwarded by the requested FIU, nor does it provide for sanctions in case of unjustified refusal on the part of the requested FIU to forward the requested information.

77. Finally, it must be pointed out that recourse to the mechanism of cooperation between the FIUs in order to obtain information necessary for combating money laundering or terrorist financing raises specific difficulties with regard to activities carried out under the freedom to provide services.

78. First, in that context, it is the FIU of the host Member State in whose territory the criminal financial transactions are carried out which is best acquainted with the risks associated with money laundering and terrorist financing in its own country. It is aware of all the facts likely to be linked to criminal financial activity in that country, not only in relation to the credit institutions and persons referred to in Directive 2005/60, but also in relation to all the national authorities responsible for the detection and eradication of financial crime, whether the administrative, judicial or enforcement authorities or the supervisory bodies for stock markets or financial derivatives markets.

79. Secondly, to be able to carry out a request for information through the mechanism for cooperation between the FIUs provided for by Decision 2000/642, the FIU must already be in possession of information indicating suspicion of money laundering or terrorist financing. Since disclosure relating to suspicious transactions is carried out, pursuant to Article 22(2) of Directive 2005/60, at the FIU of the Member State of origin and Decision 2000/642 does not provide for the requirement to forward them automatically to the FIU of the host Member State, the latter will only rarely have information corroborating the suspicions necessary so as to send a request for information to the FIU of the Member State of origin.

80. Furthermore, while a requirement for disclosure to the FIU of the host Member State gives rise to additional expenses and administrative burdens on the part of credit institutions operating under the freedom to provide services, they are relatively limited where those credit institutions are already required to establish infrastructure necessary for information to be forwarded to the FIU of the Member State where they are situated.

81. In those circumstances, national legislation of a host Member State, such as that at issue in the main proceedings, complies with the requirement for proportionality to the extent that it requires credit institutions situated in another Member State to forward, concerning operations carried out under the freedom to provide services, information necessary for combating money laundering and terrorist financing directly to the FIU of the host Member State, only where there is no effective mechanism ensuring full and complete cooperation between the FIUs and allowing money laundering and terrorist financing to be combated just as effectively.

82. In the present case, the Spanish legislation at issue in the main proceedings requires credit institutions which carry out activities in Spain, either through branches or under the freedom to provide services without a permanent establishment, to forward directly to the Spanish FIU operations involving transfers of funds from or towards certain territories, on condition that the amount of the operations covered exceeds EUR 30,000.

83. Such legislation, which requires not that all operations in any way carried out under the freedom to provide services in Spain be communicated, but merely those which, in accordance with objective criteria laid down by the national legislature, must be considered suspicious, does not appear to be disproportionate.

84. Finally, as the Advocate General has pointed out in point 115 of his Opinion, that legislation, in so far as it subjects to its requirements all credit institutions as well as all foreign persons or bodies which carry out activities in Spain through a principal establishment, branches or under the freedom to provide services, does not appear to be discriminatory.

85. It follows from all the above considerations that the answer to the question submitted is that: – Article 22(2) of Directive 2005/60 must be interpreted as not precluding legislation of a Member State which requires credit institutions to communicate the information required for the purpose of combating money laundering and terrorist financing directly to the FIU of that Member State where the institutions carry out their activities in that State under the freedom to provide services, to the extent that that legislation does not compromise the effectiveness of that directive and of Decision 2000/642;

– Article 56 TFEU must be interpreted as not precluding such legislation if the latter is justified by overriding reasons in the public interest, secures the attainment of the aim in view and does not go beyond that which is necessary in order to attain it, and is applied in a non-discriminatory manner, which it is for the national court to ascertain taking account of the following considerations:

– such legislation is appropriate to attain the aim of preventing money laundering and terrorist financing if it enables the Member State concerned effectively to supervise and suspend suspicious financial transactions concluded by credit institutions offering their services in the national territory and, if appropriate, to pursue and punish those responsible;

– the obligation imposed by that legislation on credit institutions carrying out their activities under the freedom to provide services may constitute a proportionate measure in pursuit of that aim in the absence, at the time of the facts in the main proceedings, of any effective mechanism guaranteeing full and complete cooperation between FIUs.

Costs

86. Since these proceedings are, for the parties to the main proceedings, a step in the action, having before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

1. Article 22(2) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing must be interpreted as not precluding legislation of a Member State which requires credit institutions to communicate the information required for the purpose of combating money laundering and terrorist financing directly to the FIU of that Member State where the institutions carry out their activities in that State under the freedom to provide services, to the extent that that legislation does not compromise the effectiveness of that directive and of Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

2. Article 56 TFEU must be interpreted as not precluding such legislation if the latter is justified by overriding reasons in the public interest, secures the attainment of the aim in view and does not go beyond that which is necessary in order to attain it, and is applied in a non-discriminatory manner, which it is for the national court to ascertain taking account of the following considerations:

– such legislation is appropriate to attain the aim of preventing money laundering and terrorist financing if it
enables the Member State concerned effectively to supervise and suspend suspicious financial transactions concluded by credit institutions offering their services in the national territory and, if appropriate, to pursue and punish those responsible;
- the obligation imposed by that legislation on credit institutions carrying out their activities under the freedom to provide services may constitute a proportionate measure in pursuit of that aim in the absence, at the time of the facts in the main proceedings, of any effective mechanism guaranteeing full and complete cooperation between financial intelligence units.

[Signatures]

* Language of the case: Spanish.
XI. Jurisdiction

Council regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) –

(!!) REPEALED since 10th of January 2015

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 61(c) and Article 67(1) thereof,
Having regard to the proposal from the Commission
Having regard to the opinion of the European Parliament (2),
Having regard to the opinion of the Economic and Social Committee (3),

Whereas:

(1) The Community has set itself the objective of maintaining and developing an area of freedom, security and justice, in which the free movement of persons is ensured. In order to establish progressively such an area, the Community should adopt, amongst other things, the measures relating to judicial cooperation in civil matters which are necessary for the sound operation of the internal market.

(2) Certain differences between national rules governing jurisdiction and recognition of judgments hamper the sound operation of the internal market. Provisions to unify the rules of conflict of jurisdiction in civil and commercial matters and to simplify the formalities with a view to rapid and simple recognition and enforcement of judgments from Member States bound by this Regulation are essential.

(3) This area is within the field of judicial cooperation in civil matters within the meaning of Article 65 of the Treaty.

(4) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objectives of this Regulation cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community. This Regulation confines itself to the minimum required in order to achieve those objectives and does not go beyond what is necessary for that purpose.

(5) On 27 September 1968 the Member States, acting under Article 293, fourth indent, of the Treaty, concluded the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, as amended by Conventions on the Accession of the New Member States to that Convention (hereinafter referred to as the 'Brussels Convention') (4). On 16 September 1988 Member States and EFTA States concluded the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, which is a parallel Convention to the 1968 Brussels Convention. Work has been undertaken for the revision of those Conventions, and the Council has approved the content of the revised texts. Continuity in the results achieved in that revision should be ensured.

(6) In order to attain the objective of free movement of judgments in civil and commercial matters, it is necessary and appropriate that the rules governing jurisdiction and the recognition and enforcement of judgments be governed by a Community legal instrument which is binding and directly applicable.

(7) The scope of this Regulation must cover all the main civil and commercial matters apart from certain well-defined matters.

(8) There must be a link between proceedings to which this Regulation applies and the territory of the Member States bound by this Regulation. Accordingly common rules on jurisdiction should, in principle, apply when the defendant is domiciled in one of those Member States.

(9) A defendant not domiciled in a Member State is in general subject to national rules of jurisdiction applicable in the territory of the Member State of the court seised, and a defendant domiciled in a Member State not bound by this Regulation must remain subject to the Brussels Convention.

(10) For the purposes of the free movement of judgments, judgments given in a Member State bound by this Regulation should be recognised and enforced in another Member State bound by this Regulation, even if the judgment debtor is domiciled in a third State.

(11) The rules of jurisdiction must be highly predictable and founded on the principle that jurisdiction is generally based on the defendant's domicile and jurisdiction must always be available on this ground save in a few well-defined situations in which the subject-matter of the litigation or the autonomy of the parties warrants a different linking factor. The domicile of a legal person must be defined autonomously so as to make the common rules more transparent and avoid conflicts of jurisdiction.

(12) In addition to the defendant’s domicile, there should be alternative grounds of jurisdiction based on a close link between the court and the action or in order to facilitate the sound administration of justice.

(13) In relation to insurance, consumer contracts and employment, the weaker party should be protected by rules of jurisdiction more favourable to his interests than the general rules provide for.

(14) The autonomy of the parties to a contract, other than an insurance, consumer or employment contract, where only limited autonomy to determine the courts having jurisdiction is allowed, must be respected subject to the exclusive grounds of jurisdiction laid down in this Regulation.

(15) In the interests of the harmonious administration of justice it is necessary to minimise the possibility of concurrent proceedings and to ensure that irreconcilable judgments will not be given in two Member States. There must be a clear and effective mechanism for resolving cases of lis pendens and related actions and for obviating problems...
flowing from national differences as to the determination of the time when a case is regarded as pending. For the purposes of this Regulation that time should be defined autonomously.

(16) Mutual trust in the administration of justice in the Community justifies judgments given in a Member State being recognised automatically without the need for any procedure except in cases of dispute.

(17) By virtue of the same principle of mutual trust, the procedure for making enforceable in one Member State a judgment given in another must be efficient and rapid. To that end, the declaration that a judgment is enforceable should be issued virtually automatically after purely formal checks of the documents supplied, without there being any possibility for the court to raise of its own motion any of the grounds for non-enforcement provided for by this Regulation.

(18) However, respect for the rights of the defence means that the defendant should be able to appeal in an adversarial procedure, against the declaration of enforceability, if he considers one of the grounds for non-enforcement to be present. Redress procedures should also be available to the claimant where his application for a declaration of enforceability has been rejected.

(19) Continuity between the Brussels Convention and this Regulation should be ensured, and transitional provisions should be laid down to that end. The same need for continuity applies as regards the interpretation of the Brussels Convention by the Court of Justice of the European Communities and the 1971 Protocol (5) should remain applicable also to cases already pending when this Regulation enters into force.

(20) The United Kingdom and Ireland, in accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, have given notice of their wish to take part in the adoption and application of this Regulation.

(21) Denmark, in accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty establishing the European Community, is not participating in the adoption of this Regulation, and is therefore not bound by it nor subject to its application.

(22) Since the Brussels Convention remains in force in relations between Denmark and the Member States that are bound by this Regulation, both the Convention and the 1971 Protocol continue to apply between Denmark and the Member States bound by this Regulation.

(23) The Brussels Convention also continues to apply to the territories of the Member States which fall within the territorial scope of that Convention and which are excluded from this Regulation pursuant to Article 299 of the Treaty.

(24) Likewise for the sake of consistency, this Regulation should not affect rules governing jurisdiction and the recognition of judgments contained in specific Community instruments.

(25) Respect for international commitments entered into by the Member States means that this Regulation should not affect conventions relating to specific matters to which the Member States are parties.

(26) The necessary flexibility should be provided for in the basic rules of this Regulation in order to take account of the specific procedural rules of certain Member States. Certain provisions of the Protocol annexed to the Brussels Convention should accordingly be incorporated in this Regulation.

(27) In order to allow a harmonious transition in certain areas which were the subject of special provisions in the Protocol annexed to the Brussels Convention, this Regulation lays down, for a transitional period, provisions taking into consideration the specific situation in certain Member States.

(28) No later than five years after entry into force of this Regulation the Commission will present a report on its application and, if need be, submit proposals for adaptations.

(29) The Commission will have to adjust Annexes I to IV on the rules of national jurisdiction, the courts or competent authorities and redress procedures available on the basis of the amendments forwarded by the Member State concerned; amendments made to Annexes V and VI should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (6).

HAS ADOPTED THIS REGULATION:

CHAPTER I

SCOPE

Article 1
1. This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. It shall not extend, in particular, to revenue, customs or administrative matters.

2. The Regulation shall not apply to:

(a) the status or legal capacity of natural persons, rights in property arising out of a matrimonial relationship, wills and succession;

(b) bankruptcy, proceedings relating to the winding-up of insolvent companies or other legal persons, judicial arrangements, compositions and analogous proceedings;

(c) social security;

(d) arbitration.

3. In this Regulation, the term 'Member State' shall mean Member States with the exception of Denmark.

CHAPTER II

JURISDICTION

Section 1

General provisions

Article 2
1. Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.

2. Persons who are not nationals of the Member State in which they are domiciled shall be governed by the rules of jurisdiction applicable to nationals of that State.

Article 3
1. Persons domiciled in a Member State may be sued in the courts of another Member State only by virtue of the rules set out in Sections 2 to 7 of this Chapter.

2. In particular the rules of national jurisdiction set out in Annex I shall not be applicable as against them.

Article 4
1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State.
2. As against such a defendant, any person domiciled in a Member State may, whatever his nationality, avail himself in that State of the rules of jurisdiction there in force, and in particular those specified in Annex I, in the same way as the nationals of that State.

Section 2
Special jurisdiction

Article 5
A person domiciled in a Member State may, in another Member State, be sued:

1. (a) in matters relating to a contract, in the courts for the place of performance of the obligation in question;

(b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be:

— in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered,

— in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided;

(c) if subparagraph (b) does not apply then subparagraph (a) applies;

2. in matters relating to maintenance, in the courts for the place where the maintenance creditor is domiciled or habitually resident or, if the matter is ancillary to proceedings concerning the status of a person, in the court which, according to its own law, has jurisdiction to entertain those proceedings, unless that jurisdiction is based solely on the nationality of one of the parties;

3. in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur;

4. as regards a civil claim for damages or restitution which is based on an act giving rise to criminal proceedings, in the court seised of those proceedings, to the extent that that court has jurisdiction under its own law to entertain civil proceedings;

5. as regards a dispute arising out of the operations of a branch, agency or other establishment, in the courts for the place in which the branch, agency or other establishment is situated;

6. as settlor, trustee or beneficiary of a trust created by the operation of a statute, or by a written instrument, or created orally and evidenced in writing, in the courts of the Member State in which the trust is domiciled;

7. as regards a dispute concerning the payment of remuneration claimed in respect of the salvage of a cargo or freight, in the court under the authority of which the cargo or freight in question:

(a) has been arrested to secure such payment, or

(b) could have been so arrested, but bail or other security has been given;

provided that this provision shall apply only if it is claimed that the defendant has an interest in the cargo or freight or had such an interest at the time of salvage.

Article 6
A person domiciled in a Member State may also be sued:

1. where he is one of a number of defendants, in the courts for the place where any one of them is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings;

2. as a third party in an action on a warranty or guarantee or in any other third party proceedings, in the court seised of the original proceedings, unless these were instituted solely with the object of removing him from the jurisdiction of the court which would be competent in his case;

3. on a counter-claim arising from the same contract or facts on which the original claim was based, in the court in which the original claim is pending;

4. in matters relating to a contract, if the action may be combined with an action against the same defendant in matters relating to rights in rem in immovable property, in the court of the Member State in which the property is situated.

Article 7
Where by virtue of this Regulation a court of a Member State has jurisdiction in actions relating to liability from the use or operation of a ship, that court, or any other court substituted for this purpose by the internal law of that Member State, shall also have jurisdiction over claims for limitation of such liability.

Section 3
Jurisdiction in matters relating to insurance

Article 8
In matters relating to insurance, jurisdiction shall be determined by this Section, without prejudice to Article 4 and point 5 of Article 5.

Article 9
1. An insurer domiciled in a Member State may be sued:

(a) in the courts of the Member State where he is domiciled, or

(b) in another Member State, in the case of actions brought by the policyholder, the insured or a beneficiary, in the courts for the place where the plaintiff is domiciled;

(c) if he is a co-insurer, in the courts of a Member State in which proceedings are brought against the leading insurer.

2. An insurer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

Article 10
In respect of liability insurance or insurance of immovable property, the insurer may in addition be sued in the courts
for the place where the harmful event occurred. The same applies if movable and immovable property are covered by the same insurance policy and both are adversely affected by the same contingency.

Article 11
1. In respect of liability insurance, the insurer may also, if the law of the court permits it, be joined in proceedings which the injured party has brought against the insured.

2. Articles 8, 9 and 10 shall apply to actions brought by the injured party directly against the insurer, where such direct actions are permitted.

3. If the law governing such direct actions provides that the policyholder or the insured may be joined as a party to the action, the same court shall have jurisdiction over them.

Article 12
1. Without prejudice to Article 11(3), an insurer may bring proceedings only in the courts of the Member State in which the defendant is domiciled, irrespective of whether he is the policyholder, the insured or a beneficiary.

2. The provisions of this Section shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 13
The provisions of this Section may be departed from only by an agreement:

1. which is entered into after the dispute has arisen, or

2. which allows the policyholder, the insured or a beneficiary to bring proceedings in courts other than those indicated in this Section, or

3. which is concluded between a policyholder and an insurer, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which has the effect of conferring jurisdiction on the courts of that State even if the harmful event were to occur abroad, provided that such an agreement is not contrary to the law of that State, or

4. which is concluded with a policyholder who is not domiciled in a Member State, except in so far as the insurance is compulsory or relates to immovable property in a Member State, or

5. which relates to a contract of insurance in so far as it covers one or more of the risks set out in Article 14.

Article 14
The following are the risks referred to in Article 13(5):

1. any loss of or damage to:
   (a) seagoing ships, installations situated offshore or on the high seas, or aircraft, arising from perils which relate to their use for commercial purposes;
   (b) goods in transit other than passengers’ baggage where the transit consists of or includes carriage by such ships or aircraft;
   2. any liability, other than for bodily injury to passengers or loss of or damage to their baggage:
   (a) arising out of the use or operation of ships, installations or aircraft as referred to in point 1(a) in so far as, in respect of the latter, the law of the Member State in which such aircraft are registered does not prohibit agreements on jurisdiction regarding insurance of such risks;
   (b) for loss or damage caused by goods in transit as described in point 1(b);
   3. any financial loss connected with the use or operation of ships, installations or aircraft as referred to in point 1(a), in particular loss of freight or charter-hire;
   4. any risk or interest connected with any of those referred to in points 1 to 3;
   5. notwithstanding points 1 to 4, all 'large risks' as defined in Council Directive 73/239/EEC (7), as amended by Council Directives 88/357/EEC (8) and 90/618/EEC (9), as they may be amended.

Section 4
Jurisdiction over consumer contracts

Article 15
1. In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 4 and point 5 of Article 5, if:

   (a) it is a contract for the sale of goods on instalment credit terms; or
   (b) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or
   (c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer’s domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.

2. Where a consumer enters into a contract with a party who is not domiciled in the Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that State.

3. This Section shall not apply to a contract of transport other than a contract which, for an inclusive price, provides for a combination of travel and accommodation.

Article 16
1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.

2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

3. This Article shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 17

The provisions of this Section may be departed from only by an agreement:

1. which is entered into after the dispute has arisen; or
2. which allows the consumer to bring proceedings in courts other than those indicated in this Section; or
3. which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts of that Member State, provided that such an agreement is not contrary to the law of that Member State.

Section 5

Jurisdiction over individual contracts of employment

Article 18

1. In matters relating to individual contracts of employment, jurisdiction shall be determined by this Section, without prejudice to Article 4 and point 5 of Article 5.

2. Where an employee enters into an individual contract of employment with an employer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, the employer shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

Article 19

An employer domiciled in a Member State may be sued:

1. in the courts of the Member State where he is domiciled; or
2. in another Member State:
   
   (a) in the courts for the place where the employee habitually carries out his work or in the courts for the last place where he did so, or
   
   (b) if the employee does not or did not habitually carry out his work in any one country, in the courts for the place where the business which engaged the employee is or was situated.

Article 20

1. An employer may bring proceedings only in the courts of the Member State in which the employee is domiciled.

2. The provisions of this Section shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 21

The provisions of this Section may be departed from only by an agreement on jurisdiction:

1. which is entered into after the dispute has arisen; or
2. which allows the employee to bring proceedings in courts other than those indicated in this Section.

Section 6

Exclusive jurisdiction

Article 22

The following courts shall have exclusive jurisdiction, regardless of domicile:

1. in proceedings which have as their object rights in rem in immovable property or tenancies of immovable property, the courts of the Member State in which the property is situated.

However, in proceedings which have as their object tenancies of immovable property concluded for temporary private use for a maximum period of six consecutive months, the courts of the Member State in which the defendant is domiciled shall also have jurisdiction, provided that the tenant is a natural person and that the landlord and the tenant are domiciled in the same Member State;

2. in proceedings which have as their object the validity of the constitution, the nullity or the dissolution of companies or other legal persons or associations of natural or legal persons, or of the validity of the decisions of their organs, the courts of the Member State in which the company, legal person or association has its seat. In order to determine that seat, the court shall apply its rules of private international law;

3. in proceedings which have as their object the validity of entries in public registers, the courts of the Member State in which the register is kept;

4. in proceedings concerned with the registration or validity of patents, trade marks, designs, or other similar rights required to be deposited or registered, the courts of the Member State in which the deposit or registration has been applied for, has taken place or is under the terms of a Community instrument or an international convention deemed to have taken place.

Without prejudice to the jurisdiction of the European Patent Office under the Convention on the Grant of European Patents, signed at Munich on 5 October 1973, the courts of each Member State shall have exclusive jurisdiction, regardless of domicile, in proceedings concerned with the registration or validity of any European patent granted for that State;

5. in proceedings concerned with the enforcement of judgments, the courts of the Member State in which the judgment has been or is to be enforced.

Section 7

Prorogation of jurisdiction

Article 23

1. If the parties, one or more of whom is domiciled in a Member State, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction. Such jurisdiction shall be exclusive unless the parties have agreed otherwise. Such an agreement conferring jurisdiction shall be either:

   (a) in writing or evidenced in writing; or
   
   (b) in a form which accords with practices which the parties have established between themselves; or

   (c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to...
have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.

2. Any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'.

3. Where such an agreement is concluded by parties, none of whom is domiciled in a Member State, the courts of other Member States shall have no jurisdiction over their disputes unless the court or courts chosen have declined jurisdiction.

4. The court or courts of a Member State on which a trust instrument has conferred jurisdiction shall have exclusive jurisdiction in any proceedings brought against a settlor, trustee or beneficiary, if relations between these persons or their rights or obligations under the trust are involved.

5. Agreements or provisions of a trust instrument conferring jurisdiction shall have no legal force if they are contrary to Articles 13, 17 or 21, or if the courts whose jurisdiction they purport to exclude have exclusive jurisdiction by virtue of Article 22.

Article 24
Apart from jurisdiction derived from other provisions of this Regulation, a court of a Member State before which a defendant enters an appearance shall have jurisdiction. This rule shall not apply where appearance was entered to contest the jurisdiction, or where another court has exclusive jurisdiction by virtue of Article 22.

Section 8
Examination as to jurisdiction and admissibility

Article 25
Where a court of a Member State is seised of a claim which is principally concerned with a matter over which the courts of another Member State have exclusive jurisdiction by virtue of Article 22, it shall declare of its own motion that it has no jurisdiction.

Article 26
1. Where a defendant domiciled in one Member State is sued in a court of another Member State and does not enter an appearance, the court shall declare of its own motion that it has no jurisdiction unless its jurisdiction is derived from the provisions of this Regulation.

2. The court shall stay the proceedings so long as it is not shown that the defendant has been able to receive the document instituting the proceedings or an equivalent document in sufficient time to enable him to arrange for his defence, or that all necessary steps have been taken to this end.

3. Article 19 of Council Regulation (EC) No 1348/2000 of 29 May 2000 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (10) shall apply instead of the provisions of paragraph 2 if the document instituting the proceedings or an equivalent document had to be transmitted from one Member State to another pursuant to this Regulation.

4. Where the provisions of Regulation (EC) No 1348/2000 are not applicable, Article 15 of the Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters shall apply if the document instituting the proceedings or an equivalent document had to be transmitted pursuant to that Convention.

Section 9
Lis pendens — related actions

Article 27
1. Where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established.

2. Where the jurisdiction of the court first seised is established, any court other than the court first seised shall decline jurisdiction in favour of that court.

Article 28
1. Where related actions are pending in the courts of different Member States, any court other than the court first seised may stay its proceedings.

2. Where these actions are pending at first instance, any court other than the court first seised may also, on the application of one of the parties, decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.

3. For the purposes of this Article, actions are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

Article 29
Where actions come within the exclusive jurisdiction of several courts, any court other than the court first seised shall decline jurisdiction in favour of that court.

Article 30
For the purposes of this Section, a court shall be deemed to be seised:

1. at the time when the document instituting the proceedings or an equivalent document is lodged with the court, provided that the plaintiff has not subsequently failed to take the steps he was required to take to have service effected on the defendant, or

2. if the document has to be served before being lodged with the court, at the time when it is received by the authority responsible for service, provided that the plaintiff has not subsequently failed to take the steps he was required to take to have the document lodged with the court.

Section 10
Provisional, including protective, measures

Article 31
Application may be made to the courts of a Member State for such provisional, including protective, measures as may be available under the law of that State, even if, under this Regulation, the courts of another Member State have jurisdiction as to the substance of the matter.

CHAPTER III
RECOGNITION AND ENFORCEMENT

Article 32
For the purposes of this Regulation, ‘judgment’ means any judgment given by a court or tribunal of a Member State, whatever the judgment may be called, including a decree, order, decision or writ of execution, as well as the determination of costs or expenses by an officer of the court.
Section 1
Recognition

Article 33
1. A judgment given in a Member State shall be recognised in the other Member States without any special procedure being required.

2. Any interested party who raises the recognition of a judgment as the principal issue in a dispute may, in accordance with the procedures provided for in Sections 2 and 3 of this Chapter, apply for a decision that the judgment be recognised.

3. If the outcome of proceedings in a court of a Member State depends on the determination of an incidental question of recognition that court shall have jurisdiction over that question.

Article 34
A judgment shall not be recognised:

1. if such recognition is manifestly contrary to public policy in the Member State in which recognition is sought;

2. where it was given in default of appearance, if the defendant was not served with the document which instituted the proceedings or with an equivalent document in sufficient time and in such a way as to enable him to arrange for his defence, unless the defendant failed to commence proceedings to challenge the judgment when it was possible for him to do so;

3. if it is irreconcilable with a judgment given in a dispute between the same parties in the Member State in which recognition is sought;

4. if it is irreconcilable with an earlier judgment given in another Member State or in a third State involving the same cause of action and between the same parties, provided that the earlier judgment fulfils the conditions necessary for its recognition in the Member State addressed.

Article 35
1. Moreover, a judgment shall not be recognised if it conflicts with Sections 3, 4 or 6 of Chapter II, or in a case provided for in Article 72.

2. In its examination of the grounds of jurisdiction referred to in the foregoing paragraph, the court or authority applied to shall be bound by the findings of fact on which the court in the Member State of origin based its jurisdiction.

3. Subject to the paragraph 1, the jurisdiction of the court of the Member State of origin may not be reviewed. The test of public policy referred to in point 1 of Article 34 may not be applied to the rules relating to jurisdiction.

Article 36
Under no circumstances may a foreign judgment be reviewed as to its substance.

Article 37
1. A court of a Member State in which recognition is sought of a judgment given in another Member State may stay the proceedings if an ordinary appeal against the judgment has been lodged.

2. A court of a Member State in which recognition is sought of a judgment given in Ireland or the United Kingdom may stay the proceedings if enforcement is suspended in the State of origin, by reason of an appeal.

Section 2
Enforcement

Article 38
1. A judgment given in a Member State and enforceable in that State shall be enforced in another Member State when, on the application of any interested party, it has been declared enforceable there.

2. However, in the United Kingdom, such a judgment shall be enforced in England and Wales, in Scotland, or in Northern Ireland when, on the application of any interested party, it has been registered for enforcement in that part of the United Kingdom.

Article 39
1. The application shall be submitted to the court or competent authority indicated in the list in Annex II.

2. The local jurisdiction shall be determined by reference to the place of domicile of the party against whom enforcement is sought, or to the place of enforcement.

Article 40
1. The procedure for making the application shall be governed by the law of the Member State in which enforcement is sought.

2. The applicant must give an address for service of process within the area of jurisdiction of the court applied to. However, if the law of the Member State in which enforcement is sought does not provide for the furnishing of such an address, the applicant shall appoint a representative ad litem.

3. The documents referred to in Article 53 shall be attached to the application.

Article 41
The judgment shall be declared enforceable immediately on completion of the formalities in Article 53 without any review under Articles 34 and 35. The party against whom enforcement is sought shall not at this stage of the proceedings be entitled to make any submissions on the application.

Article 42
1. The decision on the application for a declaration of enforceability shall forthwith be brought to the notice of the applicant in accordance with the procedure laid down by the law of the Member State in which enforcement is sought.

2. The declaration of enforceability shall be served on the party against whom enforcement is sought, accompanied by the judgment, if not already served on that party.

Article 43
1. The decision on the application for a declaration of enforceability may be appealed against by either party.

2. The appeal is to be lodged with the court indicated in the list in Annex III.

3. The appeal shall be dealt with in accordance with the rules governing procedure in contradictory matters.

4. If the party against whom enforcement is sought fails to appear before the appellate court in proceedings concerning an appeal brought by the applicant, Article 26(2) to (4) shall apply even where the party against whom enforcement is sought is not domiciled in any of the Member States.
5. An appeal against the declaration of enforceability is to be lodged within one month of service thereof. If the party against whom enforcement is sought is domiciled in a Member State other than that in which the declaration of enforceability was given, the time for appealing shall be two months and shall run from the date of service, either on him in person or at his residence. No extension of time may be granted on account of distance.

Article 44
The judgment given on the appeal may be contested only by the appeal referred to in Annex IV.

Article 45
1. The court with which an appeal is lodged under Article 43 or Article 44 shall refuse or revoke a declaration of enforceability only on one of the grounds specified in Articles 34 and 35. It shall give its decision without delay.

2. Under no circumstances may the foreign judgment be reviewed as to its substance.

Article 46
1. The court with which an appeal is lodged under Article 43 or Article 44 may, on the application of the party against whom enforcement is sought, stay the proceedings if an ordinary appeal has been lodged against the judgment in the Member State of origin or if the time for such an appeal has not yet expired; in the latter case, the court may specify the time within which such an appeal is to be lodged.

2. Where the judgment was given in Ireland or the United Kingdom, any form of appeal available in the Member State of origin shall be treated as an ordinary appeal for the purposes of paragraph 1.

3. The court may also make enforcement conditional on the provision of such security as it shall determine.

Article 47
1. When a judgment must be recognised in accordance with this Regulation, nothing shall prevent the applicant from availing himself of provisional, including protective, measures in accordance with the law of the Member State requested without a declaration of enforceability under Article 41 being required.

2. The declaration of enforceability shall carry with it the power to proceed to any protective measures.

3. During the time specified for an appeal pursuant to Article 43(5) against the declaration of enforceability and until any such appeal has been determined, no measures of enforcement may be taken other than protective measures against the property of the party against whom enforcement is sought.

Article 48
1. Where a foreign judgment has been given in respect of several matters and the declaration of enforceability cannot be given for all of them, the court or competent authority shall give it for one or more of them.

2. An applicant may request a declaration of enforceability limited to parts of a judgment.

Article 49
A foreign judgment which orders a periodic payment by way of a penalty shall be enforceable in the Member State in which enforcement is sought only if the amount of the payment has been finally determined by the courts of the Member State of origin.

Article 50
An applicant who, in the Member State of origin has benefited from complete or partial legal aid or exemption from costs or expenses, shall be entitled, in the procedure provided for in this Section, to benefit from the most favourable legal aid or the most extensive exemption from costs or expenses provided for by the law of the Member State addressed.

Article 51
No security, bond or deposit, however described, shall be required of a party who in one Member State applies for enforcement of a judgment given in another Member State on the ground that he is a foreign national or that he is not domiciled or resident in the State in which enforcement is sought.

Article 52
In proceedings for the issue of a declaration of enforceability, no charge, duty or fee calculated by reference to the value of the matter at issue may be levied in the Member State in which enforcement is sought.

Section 3
Common provisions

Article 53
1. A party seeking recognition or applying for a declaration of enforceability shall produce a copy of the judgment which satisfies the conditions necessary to establish its authenticity.

2. A party applying for a declaration of enforceability shall also produce the certificate referred to in Article 54, without prejudice to Article 55.

Article 54
The court or competent authority of a Member State where a judgment was given shall issue, at the request of any interested party, a certificate using the standard form in Annex V to this Regulation.

Article 55
1. If the certificate referred to in Article 54 is not produced, the court or competent authority may specify a time for its production or accept an equivalent document or, if it considers that it has sufficient information before it, dispense with its production.

2. If the court or competent authority so requires, a translation of the documents shall be produced. The translation shall be certified by a person qualified to do so in one of the Member States.

Article 56
No legalisation or other similar formality shall be required in respect of the documents referred to in Article 53 or Article 55(2), or in respect of a document appointing a representative ad litem.

CHAPTER IV
AUTHENTIC INSTRUMENTS AND COURT SETTLEMENTS

Article 57
1. A document which has been formally drawn up or registered as an authentic instrument and is enforceable in one Member State shall, in another Member State, be declared enforceable there, on application made in accordance with the procedures provided for in Articles 38, et seq. The court with which an appeal is lodged under Article 43 or Article 44 shall refuse or revoke a declaration of
enforceability only if enforcement of the instrument is manifestly contrary to public policy in the Member State addressed.

2. Arrangements relating to maintenance obligations concluded with administrative authorities or authenticated by them shall also be regarded as authentic instruments within the meaning of paragraph 1.

3. The instrument produced must satisfy the conditions necessary to establish its authenticity in the Member State of origin.

4. Section 3 of Chapter III shall apply as appropriate. The competent authority of a Member State where an authentic instrument was drawn up or registered shall issue, at the request of any interested party, a certificate using the standard form in Annex VI to this Regulation.

Article 58
A settlement which has been approved by a court in the course of proceedings and is enforceable in the Member State in which it was concluded shall be enforceable in the State addressed under the same conditions as authentic instruments. The court or competent authority of a Member State where a court settlement was approved shall issue, at the request of any interested party, a certificate using the standard form in Annex V to this Regulation.

CHAPTER V
GENERAL PROVISIONS

Article 59
1. In order to determine whether a party is domiciled in the Member State whose courts are seised of a matter, the court shall apply its internal law.

2. If a party is not domiciled in the Member State whose courts are seised of the matter, then, in order to determine whether the party is domiciled in another Member State, the court shall apply the law of that Member State.

Article 60
1. For the purposes of this Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its:

(a) statutory seat, or
(b) central administration, or
(c) principal place of business.

2. For the purposes of the United Kingdom and Ireland ‘statutory seat’ means the registered office or, where there is no such office anywhere, the place of incorporation or, where there is no such place anywhere, the place under the law of which the formation took place.

3. In order to determine whether a trust is domiciled in the Member State whose courts are seised of the matter, the court shall apply its rules of private international law.

Article 61
Without prejudice to any more favourable provisions of national laws, persons domiciled in a Member State who are being prosecuted in the criminal courts of another Member State of which they are not nationals for an offence which was not intentionally committed may be defended by persons qualified to do so, even if they do not appear in person. However, the court seised of the matter may order appearance in person; in the case of failure to appear, a judgment given in the civil action without the person concerned having had the opportunity to arrange for his defence need not be recognised or enforced in the other Member States.

Article 62
In Sweden, in summary proceedings concerning orders to pay (betalningsföreläggande) and assistance (handräckning), the expression ‘court’ includes the ‘Swedish enforcement service’ (kronofogdemyndighet).

Article 63
1. A person domiciled in the territory of the Grand Duchy of Luxembourg and sued in the court of another Member State pursuant to Article 5(1) may refuse to submit to the jurisdiction of that court if the final place of delivery of the goods or provision of the services is in Luxembourg.

2. Where, under paragraph 1, the final place of delivery of the goods or provision of the services is in Luxembourg, any agreement conferring jurisdiction must, in order to be valid, be accepted in writing or evidenced in writing within the meaning of Article 23(1)(a).

3. The provisions of this Article shall not apply to contracts for the provision of financial services.

4. The provisions of this Article shall apply for a period of six years from entry into force of this Regulation.

Article 64
1. In proceedings involving a dispute between the master and a member of the crew of a seagoing ship registered in Greece or in Portugal, concerning remuneration or other conditions of service, a court in a Member State shall establish whether the diplomatic or consular officer responsible for the ship has been notified of the dispute. It may act as soon as that officer has been notified.

2. The provisions of this Article shall apply for a period of six years from entry into force of this Regulation.

Article 65
1. The jurisdiction specified in Article 6(2) and Article 11 in actions on a warranty of guarantee or in any other third party proceedings may not be resorted to Germany, Austria and Hungary. Any person domiciled in another Member State may be sued in the courts:

(a) of Germany, pursuant to Articles 68 and 72 to 74 of the Code of Civil Procedure (Zivilprozessordnung) concerning third-party notices;

(b) of Austria, pursuant to Article 21 of the Code of Civil Procedure (Zivilprozessordnung) concerning third-party notices;

(c) of Hungary, pursuant to Articles 58 to 60 of the Code of Civil Procedure (Polgári perrendaktárás) concerning third-party notices.

2. Judgments given in other Member States by virtue of Article 6(2), or Article 11 shall be recognised and enforced in Germany, Austria and Hungary in accordance with Chapter III. Any effects which judgments given in these States may have on third parties by application of the provisions in paragraph 1 shall also be recognised in the other Member States.

CHAPTER VI
TRANSITIONAL PROVISIONS

Article 66
1. This Regulation shall apply only to legal proceedings instituted and to documents formally drawn up or registered as authentic instruments after the entry into force thereof.
2. However, if the proceedings in the Member State of origin were instituted before the entry into force of this Regulation, judgments given after that date shall be recognised and enforced in accordance with Chapter III,
(a) if the proceedings in the Member State of origin were instituted after the entry into force of the Brussels or the Lugano Convention both in the Member State of origin and in the Member State addressed;
(b) in all other cases, if jurisdiction was founded upon rules which accorded with those provided for either in Chapter II or in a convention concluded between the Member State of origin and the Member State addressed which was in force when the proceedings were instituted.
Relevant Case Law on the repealed council regulation no 44/2001

C-478/12 Maletic

Circumstances:
11. The Maletics are domiciled in Bludesch (Austria), which lies within the jurisdiction of the Bezirksgericht Bludenz (District Court, Bludenz). On 30 December 2011, they booked and paid for themselves, as private individuals, a package holiday to Egypt on the website of lastminute.com for EUR 1 958 from 10 to 24 January 2012. On its website, lastminute.com, a company whose registered office is in Munich (Germany), stated that it acted as the travel agent and that the trip would be operated by TUI, which has its registered office in Vienna (Austria).
12. The booking made by the applicants in the main proceedings concerned the Jaz Makadi Golf & Spa hotel in Hurghada (Egypt). That booking was confirmed by lastminute.com, which passed it on to TUI. Subsequently, the Maletics received a 'confirmation/invoice' of 5 January 2012 from TUI which, while it confirmed the information concerning the trip booked with lastminute.com, mentioned the name of another hotel, the Jaz Makadi Star Resort Spa in Hurghada.
13. It was only on their arrival in Hurghada that the applicants in the main proceedings noticed the mistake concerning the hotel and paid a surcharge of EUR 1 036 to be able to stay in the hotel initially booked on lastminute.com’s website.
14. On 13 April 2012, in order to recover the surcharge paid and to be compensated for the inconvenience which affected their holiday, the applicants in the main proceedings brought an action before the Bezirksgericht Bludenz seeking payment from lastminute.com and TUI, jointly and severally of the sum of EUR 1 201.38 together with interest and costs.
21. In those circumstances, the Landgericht Feldkirch (Regional Court, Feldkirch) decided to stay the proceedings before it and to refer the following question to the Court for a preliminary ruling:

Preliminary question:
‘Is Article 16(1) of [Regulation No 44/2001], which confers jurisdiction on the courts for the place where the consumer is domiciled, to be interpreted as meaning that, in the case where the other party to the contract (here, a travel agent having its seat abroad) has recourse to a contracting partner (here, a travel operator having its seat in the home country), Article 16(1) of Regulation No 44/2001 is, for the purpose of proceedings brought against those two parties, also applicable to the contracting partner in the home country?’

Judgement:
The concept of ‘other party to the contract’ laid down in Article 16(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning, in circumstances such as those at issue in the main proceedings, that it also covers the contracting partner of the operator with which the consumer concluded that contract and which has its registered office in the Member State in which the consumer is domiciled.

Operative part of the judgment
1. Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of an alleged infringement of personality rights by means of content placed online, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised.

2. Article 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), must be interpreted as not requiring transposition in the form of a specific conflict-of-laws rule. Nevertheless, in relation to the coordinated field, Member States must ensure that, subject to the derogations authorised in accordance with the conditions set out in Article 3(4) of Directive 2000/31, the provision of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established.

Operative part of the judgment:
1. A contract concerning a voyage by freighter, such as that at issue in the main proceedings in Case C-585/08, is a contract of transport which, for an inclusive price, provides for a combination of travel and accommodation within the meaning of Article 15(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

2. In order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be ‘directing’ its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader’s overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer’s domicile, in the sense that it was minded to conclude a contract with them.

The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader’s activity is directed to the Member
State of the consumer’s domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader’s site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.

On the other hand, the mere accessibility of the trader’s or the intermediary’s website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established.

**Case C-523/10, Wintersteiger AG v Products 4U Sondermaschinenbau GmbH,**

Operative part of the judgment:

Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that an action relating to infringement of a trade mark registered in a Member State because of the use, by an advertiser, of a keyword identical to that trade mark on a search engine website operating under a country-specific top-level domain of another Member State may be brought before either the courts of the Member State in which the trade mark is registered or the courts of the Member State of the place of establishment of the advertiser.

**Case C-170/12, Peter Pinckney v KDG Mediatech AG,**

Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of alleged infringement of copyrights protected by the Member State of the court seised, the latter has jurisdiction to hear an action to establish liability brought by the author of a work against a company established in another Member State and which has, in the latter State, reproduced that work on a material and confirming the reservation in that other language, thereby obtaining a list of vehicles corresponding to the characteristics specified.

12 After selecting the vehicle which corresponded best to her search criteria, she was directed to an offer from the defendants, Mr A. Yusufi and Mr W. Yusufi, who operate a motor vehicle retail business via Autohaus Yusufi GbR (‘Autohaus Yusufi’), a partnership established in Hamburg (Germany).

13 Wishing to obtain more information about the vehicle offered on the search platform, Ms Mühlleitner contacted the defendants, using the telephone number stated on the website of Autohaus Yusufi, which included an international dialling code. As the vehicle in question was no longer available, she was offered another vehicle, details of which were subsequently sent by email. She was also informed that her Austrian nationality would not prevent her from acquiring a vehicle from the defendants.

14 Ms Mühlleitner then went to Germany and, by a contract of sale signed on 21 September 2009 in Hamburg, bought the vehicle from Mr A. Yusufi and Mr W. Yusufi at a price of EUR 11 500, taking immediate delivery of it.

15 On her return to Austria Ms Mühlleitner discovered that the vehicle she had purchased was defective, and consequently asked the defendants to repair it.

16 When the defendants refused to repair the vehicle, Ms Mühlleitner brought proceedings in the court of her place of domicile, the Landesgericht Wels (Regional Court, Wels) (Austria), for rescission of the contract for the sale of the vehicle, which she claims to have concluded as a consumer with an undertaking directing its commercial or professional activities to Austria, a case falling within Article 15(1)(c) of the Brussels I Regulation.

17 The defendants contested Ms Mühlleitner’s status of ‘consumer’ and the international jurisdiction of the Austrian courts, arguing that the dispute should be brought before the competent German courts. They also submitted that they did not direct their activities to Austria and that Ms Mühlleitner had concluded the contract at the seat of their undertaking in Germany.

……

25 In those circumstances, the Oberster Gerichtshof decided to stay the proceedings and refer the following question to the Court for a preliminary ruling:

‘Does the application of Article 15(1)(c) of [the Brussels I Regulation] presuppose that the contract between the consumer and the undertaking has been concluded at a distance?’

……

On those grounds, the Court (Fourth Chamber) hereby rules:

Article 15(1)(c) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as not requiring the contract between the consumer and the trader to be concluded at a distance.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 67(4) and points (a), (c) and (e) of Article 81 (2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) On 21 April 2009, the Commission adopted a report on the application of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (3). The report concluded that, in general, the operation of that Regulation is satisfactory, but that it is desirable to improve the application of certain of its provisions, to further facilitate the free circulation of judgments and to further enhance access to justice. Since a number of amendments are to be made to that Regulation it should, in the interests of clarity, be recast. (2) At its meeting in Brussels on 10 and 11 December 2009, the European Council adopted a new multiannual programme entitled ‘The Stockholm Programme – an open and secure Europe serving and protecting citizens’ (4). In the Stockholm Programme the European Council considered that the process of abolishing all intermediate measures (the exequatur) should be continued during the period covered by that Programme. At the same time the abolition of the exequatur should also be accompanied by a series of safeguards. (3) The Union has set itself the objective of maintaining and developing an area of freedom, security and justice, inter alia, by facilitating access to justice, in particular through the principle of mutual recognition of judicial and extra-judicial decisions in civil matters. For the gradual establishment of such an area, the Union is to adopt measures relating to judicial cooperation in civil matters having cross-border implications, particularly when necessary for the proper functioning of the internal market. (4) Certain differences between national rules governing jurisdiction and recognition of judgments hamper the sound operation of the internal market. Provisions to unify the rules of conflict of jurisdiction in civil and commercial matters, and to ensure rapid and simple recognition and enforcement of judgments given in a Member State, are essential. (5) Such provisions fall within the area of judicial cooperation in civil matters within the meaning of Article 81 of the Treaty on the Functioning of the European Union (TFEU). (6) In order to attain the objective of free circulation of judgments in civil and commercial matters, it is necessary and appropriate that the rules governing jurisdiction and the recognition and enforcement of judgments be governed by a legal instrument of the Union which is binding and directly applicable. (7) On 27 September 1968, the then Member States of the European Communities, acting under Article 220, fourth indent, of the Treaty establishing the European Economic Community, concluded the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, subsequently amended by conventions on the accession to that Convention of new Member States (5) (‘the 1968 Brussels Convention’). On 16 September 1988, the then Member States of the European Communities and certain EFTA States concluded the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (6) (‘the 1988 Lugano Convention’), which is a parallel convention to the 1968 Brussels Convention. The 1988 Lugano Convention became applicable to Poland on 1 February 2000. (8) On 22 December 2000, the Council adopted Regulation (EC) No 44/2001, which replaces the 1968 Brussels Convention with regard to the territories of the Member States covered by the TFEU, as between the Member States except Denmark. By Council Decision 2006/325/EC (7), the Community concluded an agreement with Denmark ensuring the application of the provisions of Regulation (EC) No 44/2001 in Denmark. The 1988 Lugano Convention was revised by the Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (8), signed at Lugano on 30 October 2007 by the Community, Denmark, Iceland, Norway and Switzerland (‘the 2007 Lugano Convention’). (9) The 1968 Brussels Convention continues to apply to the territories of the Member States which fall within the territorial scope of that Convention and which are excluded from this Regulation pursuant to Article 355 of the TFEU. (10) The scope of this Regulation should cover all the main civil and commercial matters apart from certain well-defined matters, in particular maintenance obligations, which should be excluded from the scope of this Regulation following the adoption of Council Regulation (EC) No 4/2009 of 18 December 2008 on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations (9). (11) For the purposes of this Regulation, courts or tribunals of the Member States should include courts or tribunals common to several Member States, such as the Benelux Court of Justice when it exercises jurisdiction on matters falling within the scope of this Regulation. Therefore, judgments given by such courts should be recognised and enforced in accordance with this Regulation. (12) This Regulation should not apply to arbitration. Nothing in this Regulation should prevent the courts of a Member State, when seised of an action in a matter in respect of which the parties have entered into an arbitration agreement, from referring the parties to arbitration, from staying or dismissing the proceedings, or from examining whether the arbitration agreement is null and void, inoperative or incapable of being performed, in accordance with their national law. A ruling given by a court of a Member State as to whether or not an arbitration agreement is null and void, inoperative or incapable of being performed should not be subject to the rules of recognition and enforcement laid down in this Regulation, regardless of whether the court decided on this as a principal issue or as an incidental question. On the other hand, where a court of a Member State,
exercising jurisdiction under this Regulation or under national law, has determined that an arbitration agreement is null and void, inoperative or incapable of being performed, this should not preclude that court’s judgment on the substance of the matter from being recognised or, as the case may be, enforced in accordance with this Regulation. This should be without prejudice to the competence of the courts of the Member States to decide on the recognition and enforcement of arbitral awards in accordance with the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, done at New York on 10 June 1958 (the 1958 New York Convention’), which takes precedence over this Regulation. This Regulation should not apply to any action or ancillary proceedings relating to, in particular, the establishment of an arbitral tribunal, the powers of arbitrators, the conduct of an arbitration procedure or any other aspects of such a procedure, nor to any action or judgment concerning the annulment, review, appeal, recognition or enforcement of an arbitral award.

(13) There must be a connection between proceedings to which this Regulation applies and the territory of the Member States. Accordingly, common rules of jurisdiction should, in principle, apply when the defendant is domiciled in a Member State.

(14) A defendant not domiciled in a Member State should in general be subject to the national rules of jurisdiction applicable in the territory of the Member State of the court seised. However, in order to ensure the protection of consumers and employees, to safeguard the jurisdiction of the courts of the Member States in situations where they have exclusive jurisdiction and to respect the autonomy of the parties, certain rules of jurisdiction in this Regulation should apply regardless of the defendant’s domicile.

(15) The rules of jurisdiction should be highly predictable and founded on the principle that jurisdiction is generally based on the defendant’s domicile. Jurisdiction should always be available on this ground save in a few well-defined situations in which the subject-matter of the dispute or the autonomy of the parties warrants a different connecting factor. The domicile of a legal person must be defined autonomously so as to make the common rules more transparent and avoid conflicts of jurisdiction.

(16) In addition to the defendant’s domicile, there should be alternative grounds of jurisdiction based on a close connection between the court and the action or in order to facilitate the sound administration of justice. The existence of a close connection should ensure legal certainty and avoid the possibility of the defendant being sued in a court of a Member State which he could not reasonably have foreseen. This is important, particularly in disputes concerning non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.

(17) The owner of a cultural object as defined in Article 1(1) of Council Directive 93/7/EEC of 15 March 1993 on the return of cultural objects unlawfully removed from the territory of a Member State (16) may, on the grounds set out in this Regulation to initiate proceedings as regards a civil claim for the recovery, based on ownership, of such a cultural object in the courts for the place where the cultural object is situated at the time the court is seised. Such proceedings should be without prejudice to proceedings initiated under Council Directive 93/7/EEC.

(18) In relation to insurance, consumer and employment contracts, the weaker party should be protected by rules of jurisdiction more favourable to his interests than the general rules.

(19) The autonomy of the parties to a contract, other than an insurance, consumer or employment contract, where only limited autonomy to determine the courts having jurisdiction is allowed, should be respected subject to the exclusive grounds of jurisdiction laid down in this Regulation.

(20) Where a question arises as to whether a choice-of-court agreement in favour of a court or the courts of a Member State is null and void as to its substantive validity, that question should be decided in accordance with the law of the Member State of the court or courts designated in the agreement, including the conflict-of-laws rules of the Member States. There should be a clear and effective mechanism for resolving cases of lis pendens and related actions, and for obviating problems flowing from national differences as to the determination of the time when a case is regarded as pending. For the purposes of this Regulation, that time should be defined autonomously.

(21) However, in order to enhance the effectiveness of exclusive choice-of-court agreements and to avoid abusive litigation tactics, it is necessary to provide for an exception to the general lis pendens rule in order to deal satisfactorily with a particular situation in which concurrent proceedings may arise. This is the situation where a court not designated in an exclusive choice-of-court agreement has been seised of proceedings and the designated court is seised subsequently of proceedings involving the same cause of action and between the same parties. In such a case, the court first seised should be required to stay its proceedings as soon as the designated court has been seised and until such time as the latter court declares that it has no jurisdiction under the exclusive choice-of-court agreement. This is to ensure that, in such a situation, the designated court has priority to decide on the validity of the agreement and on the extent to which the agreement applies to the dispute pending before it. The designated court should be able to proceed irrespective of whether the non-designated court has already decided on the stay of proceedings.

This exception should not cover situations where the parties have entered into conflicting exclusive choice-of-court agreements or where a court designated in an exclusive choice-of-court agreement has been seised first. In such cases, the general lis pendens rule of this Regulation should apply.

(22) The Regulation should provide for a flexible mechanism allowing the courts of the Member States to take into account proceedings pending before the courts of third States, considering in particular whether a judgment of a third State will be capable of recognition and enforcement in the Member State concerned under the law of that Member State and the proper administration of justice.

(23) When taking into account the proper administration of justice, the court of the Member State concerned should assess all the circumstances of the case before it. Such circumstances may include connections between the facts of the case and the parties and the third State concerned, the stage to which the proceedings in the third State have progressed by the time proceedings are initiated in the court of the Member State and whether or not the court of the third State can be expected to give a judgment within a reasonable time.

That assessment may also include consideration of the question whether the court of the third State has exclusive jurisdiction in the particular case in circumstances where a court of a Member State would have exclusive jurisdiction.

(24) The notion of provisional, including protective,
measures should include, for example, protective orders aimed at obtaining information or preserving evidence as referred to in Articles 6 and 7 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. It should not include measures which are not of a protective nature, such as measures ordering the hearing of a witness. This should be without prejudice to the application of Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

(26) Mutual trust in the administration of justice in the Union justifies the principle that judgments given in a Member State should be recognised in all Member States without the need for any special procedure. In addition, the aim of making cross-border litigation less time-consuming and costly justifies the abolition of the declaration of enforceability prior to enforcement in the Member State addressed. As a result, a judgment given by the courts of a Member State should be treated as if it had been given in the Member State addressed.

(27) For the purposes of the free circulation of judgments, a judgment given in a Member State should be recognised and enforced in another Member State even if it is given against a person not domiciled in a Member State.

(28) Where a judgment contains a measure or order which is not known in the law of the Member State addressed, that measure or order, including any right indicated therein, should, to the extent possible, be adapted to one which, under the law of that Member State, has equivalent effects attached to it and pursues similar aims. The adaptation is to be determined by each Member State.

(29) The direct enforcement in the Member State addressed of a judgment given in another Member State without a declaration of enforceability should not jeopardise respect for the rights of the defence. Therefore, the person against whom enforcement is sought should be able to apply for refusal of the recognition or enforcement of a judgment if he considers one of the grounds for refusal of recognition to be present. This should include the ground that he had not had the opportunity to arrange for his defence where the judgment was given in default of appearance in a civil action linked to criminal proceedings. It should also include the grounds which could be invoked on the basis of an agreement between the Member State addressed and a third State concluded pursuant to Article 59 of the 1968 Brussels Convention.

(30) A party challenging the enforcement of a judgment given in another Member State should, to the extent possible and in accordance with the legal system of the Member State addressed, be able to invoke, in the same procedure, in addition to the grounds for refusal provided for in this Regulation, the grounds for refusal available under national law and within the time-limits laid down in that law. The recognition of a judgment should, however, be refused only if one or more of the grounds for refusal provided for in this Regulation are present.

(31) Pending a challenge to the enforcement of a judgment, it should be possible for the courts in the Member State addressed, during the entire proceedings relating to such a challenge, including any appeal, to allow the enforcement to proceed subject to a limitation of the enforcement or to the provision of security.

(32) In order to inform the person against whom enforcement is sought of the enforcement of a judgment given in another Member State, the certificate established under this Regulation, if necessary accompanied by the judgment, should be served on that person in reasonable time before the first enforcement measure. In this context, the first enforcement measure should mean the first enforcement measure after such service.

(33) Where provisional, including protective, measures are ordered by a court having jurisdiction as to the substance of the matter, their free circulation should be ensured under this Regulation. However, provisional, including protective, measures which were ordered by such a court without the defendant being summoned to appear should not be recognised and enforced under this Regulation unless the judgment containing the measure is served on the defendant prior to enforcement. This should not preclude the recognition and enforcement of such measures under national law. Where provisional, including protective, measures are ordered by a court of a Member State not having jurisdiction as to the substance of the matter, the effect of such measures should be confined, under this Regulation, to the territory of that Member State.

(34) Continuity between the 1968 Brussels Convention, Regulation (EC) No 44/2001 and this Regulation should be ensured, and transitional provisions should be laid down to that end. The same need for continuity applies as regards the interpretation by the Court of Justice of the European Union of the 1968 Brussels Convention and of the Regulations replacing it.

(35) Respect for international commitments entered into by the Member States addressed means that this Regulation should not affect conventions relating to specific matters to which the Member States are parties.

(36) Without prejudice to the obligations of the Member States under the Treaties, this Regulation should not affect the application of bilateral conventions and agreements between the Member States and third States concluded before the date of entry into force of Regulation (EC) No 44/2001 which concern matters governed by this Regulation.

(37) In order to ensure that the certificates to be used in connection with the recognition or enforcement of judgments, authentic instruments and court settlements under this Regulation are kept up-to-date, the power to adopt acts in accordance with Article 290 of the TFEU should be delegated to the Commission in respect of amendments to Annexes I and II to this Regulation. It is in particular important that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(38) This Regulation respects fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial guaranteed in Article 47 of the Charter.

(39) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union and of the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(40) The United Kingdom and Ireland, in accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the TEU and to the Treaty establishing the European Community, took part in the adoption and application of Regulation (EC) No 44/2001. In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, the United
CASEBOOK OF ICT LAW
2015

Kingdom and Ireland have notified their wish to take part in the adoption and application of this Regulation.

(41) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to the possibility for Denmark of applying the amendments to Regulation (EEC) No 44/2001 pursuant to Article 3 of the Agreement of 19 October 2005 between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (13).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SCOPE AND DEFINITIONS

Article 1

1. This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. It shall not extend, in particular, to revenues, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (acta iure imperii).

2. This Regulation shall not apply to:
   (a) the status or legal capacity of natural persons, rights in property arising out of a matrimonial relationship or out of a relationship deemed by the law applicable to such relationship to have comparable effects to marriage;
   (b) bankruptcy, proceedings relating to the winding-up of insolvent companies or other legal persons, judicial arrangements, compositions and analogous proceedings;
   (c) social security;
   (d) arbitration;
   (e) maintenance obligations arising from a family relationship, parentage, marriage or affinity;
   (f) wills and succession, including maintenance obligations arising by reason of death.

Article 2

For the purposes of this Regulation:
   (a) judgment means any judgment given by a court or tribunal of a Member State, whatever the judgment may be called, including a decree, order, decision or writ of execution, as well as a decision on the determination of costs or expenses by an officer of the court;
   (b) court settlement means a settlement which has been approved or concluded, or been approved or concluded, or
   (c) authentic instrument means a document which has been formally drawn up or registered as an authentic instrument in the Member State of origin and the authenticity of which:
      (i) relates to the signature and the content of the instrument; and
      (ii) has been established by a public authority or other authority empowered for that purpose;
   (d) Member State of origin means the Member State in which, as the case may be, the judgment or the court settlement has been approved or concluded, or the authentic instrument has been formally drawn up or registered;
   (e) Member State addressed means the Member State in which the recognition of the judgment is invoked or in which the enforcement of the judgment, the court settlement or the authentic instrument is sought;
   (f) court of origin means the court which has given the judgment the recognition of which is invoked or the enforcement of which is sought.

Article 3

For the purposes of this Regulation, ‘court’ includes the following authorities to the extent that they have jurisdiction in matters falling within the scope of this Regulation:
   (a) in Hungary, in summary proceedings concerning orders to pay (üzleti megnyugtató eljárás), the notary (közjegyző);
   (b) in Sweden, in summary proceedings concerning orders to pay (betalningsföreläggande) and assistance (handräkning), the Enforcement Authority (Kronofogdeynidigheten).

CHAPTER II

JURISDICTION

SECTION I

General provisions

Article 4

1. Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.

2. Persons who are not nationals of the Member State in which they are domiciled shall be governed by the rules of jurisdiction applicable to nationals of that Member State.

Article 5

1. Persons domiciled in a Member State may be sued in the courts of another Member State only by virtue of the rules set out in Sections 2 to 7 of this Chapter.

2. In particular, the rules of national jurisdiction of which the Member States are to notify the Commission pursuant to point (a) of Article 76(1) shall not be applicable as against the persons referred to in paragraph 1.

Article 6

1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Article 18(1), Article 21(2) and Articles 24 and 25, be determined by the law of that Member State.

2. As against such a defendant, any person domiciled in a Member State may, whatever his nationality, avail himself in that Member State of the rules of jurisdiction there in force, and in particular those of which the Member States are to notify the Commission pursuant to point (a) of Article 76(1), in the same way as nationals of that Member State.

SECTION II

Special jurisdiction

Article 7

A person domiciled in a Member State may be sued in another Member State:
   (1) [a] in matters relating to a contract, in the courts for the place of performance of the obligation in question;
   (b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be:
      —in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered,
      —in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided;
   (c) if point (b) does not apply then point (a) applies;
   (2) in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur;
   (3) as regards a civil claim for damages or restitution which is based on an act giving rise to criminal proceedings, in the court seized of those proceedings, to the extent that that court has jurisdiction under its own law to entertain civil proceedings;
   (4) as regards a civil claim for the recovery, based on ownership, of a cultural object as defined in point 1 of Article 1 of Directive 93/7/EEC initiated by the person claiming the right to recover such an object, in the courts;
for the place where the cultural object is situated at the
time when the court is seised;
(5) as regards a dispute arising out of the operations of a
branch, agency or other establishment, in the courts for
the place where the branch, agency or other
establishment is situated;
(6) as regards a dispute brought against a settlor, trustee or
beneficiary of a trust created by the operation of a statute,
or by a written instrument, or created orally and
evidenced in writing, in the courts of the Member State in
which the trust is domiciled;
(7) as regards a dispute concerning the payment of
remuneration claimed in respect of the salvage of a cargo or
freight, in the court under the authority of which the
cargo or freight in question:
(a) has been arrested to secure such payment; or
(b) could have been so arrested, but bail or other security
has been given;
provided that this provision shall apply only if it is claimed
that the defendant has an interest in the cargo or
freight or had such an interest at the time of salvage.

Article 8
A person domiciled in a Member State may also be sued:
(1) where he is one of a number of defendants, in the courts
for the place where any one of them is domiciled,
provided the claims are so closely connected that it is
expedient to hear and determine them together to avoid
the risk of irreconcilable judgments resulting from
separate proceedings;
(2) as a third party in an action on a warranty or guarantee or
in any other third-party proceedings, in the court seised
of the original proceedings, unless these were instituted
solely with the object of removing him from the
jurisdiction of the court which would be competent in his
case;
(3) in a counter-claim arising from the same contract or facts
on which the original claim was based, in the court in
which the original claim is pending;
(4) in matters relating to a contract, if the action may be
combined with an action against the same defendant in
matters relating to rights in rem in immovable property,
in the court of the Member State in which the property is
situated.

Article 9
Where by virtue of this Regulation a court of a Member State
has jurisdiction in actions relating to liability from the use or
operation of a ship, that court, or any other court substituted
for this purpose by the internal law of that Member State,
shall also have jurisdiction over claims for limitation of such
liability.

SECTION 3
Jurisdiction in matters relating to insurance

Article 10
In matters relating to insurance, jurisdiction shall be
determined by this Section, without prejudice to Article 6
and point 5 of Article 7.

Article 11
1. An insurer domiciled in a Member State may be sued:
(a) in the courts of the Member State in which he is
domiciled;
(b) in another Member State, in the case of actions brought
by the policyholder, the insured or a beneficiary, in the
courts for the place where the claimant is domiciled; or
(c) if he is a co-insurer, in the courts of a Member State in
which proceedings are brought against the leading
insurer.
2. An insurer who is not domiciled in a Member State but has
a branch, agency or other establishment in one of the
Member States shall, in disputes arising out of the operations
of the branch, agency or establishment, be deemed to be
domiciled in that Member State.

Article 12
In respect of liability insurance or insurance of immovable
property, the insurer may in addition be sued in the courts
for the place where the harmful event occurred. The same
applies if movable and immovable property are covered by
the same insurance policy and both are adversely affected by
the same contingency.

Article 13
1. In respect of liability insurance, the insurer may also, if
the law of the court permits it, be joined in proceedings
which the injured party has brought against the insurer.
2. Articles 10, 11 and 12 shall apply to actions brought by
the injured party directly against the insurer, where such
direct actions are permitted;
3. If the law governing such direct actions provides that the
policyholder or the insured may be joined as a party to the
action, the same court shall have jurisdiction over them.

Article 14
1. Without prejudice to Article 13(3), an insurer may bring
proceedings only in the courts of the Member State in which
the defendant is domiciled, irrespective of whether he is the
policyholder, the insured or a beneficiary.
2. The provisions of this Section shall not affect the right to
bring a counter-claim in the court in which, in accordance
with this Section, the original claim is pending.

Article 15
The provisions of this Section may be departed from only by
an agreement:
(1) which is entered into after the dispute has arisen;
(2) which allows the policyholder, the insured or a
beneficiary to bring proceedings in courts other than
those indicated in this Section;
(3) which is concluded between a policyholder and an
insurer, both of whom are at the time of conclusion of the
contract domiciled or habitually resident in the same
Member State, and which has the effect of conferring
jurisdiction on the courts of that Member State even if the
harmful event were to occur abroad, provided that such
an agreement is not contrary to the law of that Member
State;
(4) which is concluded with a policyholder who is not
domiciled in a Member State, except in so far as the
insurance is compulsory or relates to immovable
property in a Member State; or
(5) which relates to a contract of insurance in so far as it
covers one or more of the risks set out in Article 16.

Article 16
The following are the risks referred to in point 5 of Article 15:
(1) any loss or damage to:
(a) seagoing ships, installations situated offshore or on the
high seas, or aircraft, arising from perils which relate
to the use or operation of ships or aircraft;
(b) goods in transit other than passengers' baggage where
the transit consists of or includes carriage by such
ships or aircraft;
(2) any liability, other than for bodily injury to passengers or
loss or damage to their baggage:
(a) arising out of the use or operation of ships,
installations or aircraft as referred to in point 1(a) in
so far as, in respect of the latter, the law of the Member
State in which such aircraft are registered does not
prohibit agreements on jurisdiction regarding
insurance of such risks;
(b) loss or damage caused by goods in transit as
described in point 1(b);
(3) any financial loss connected with the use or operation of ships,
installations or aircraft as referred to in point 1(a), in
particular loss of freight or charter-hire;
(4) any risk or interest connected with any of those referred
to in points 1 to 3;
(5) notwithstanding points 1 to 4, all 'large risks' as defined in
and of the Council of 25 November 2009 on the taking-up
and pursuit of the business of Insurance and Reinsurance
(Solvency II) [14].

SECTION 4
Jurisdiction over consumer contracts

Article 17
1. In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 6 and point 5 of Article 7, if:
(a) it is a contract for the sale of goods on instalment credit terms;
(b) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or
(c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.
2. Where a consumer enters into a contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.
3. This Section shall not apply to a contract of transport other than a contract which, for an inclusive price, provides for a combination of travel and accommodation.

Article 18
1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled.
2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.
3. This Article shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 19
The provisions of this Section may be departed from only by an agreement:
(1) which is entered into after the dispute has arisen;
(2) which allows the consumer to bring proceedings in courts other than those indicated in this Section; or
(3) which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts of that Member State, provided that such an agreement is not contrary to the law of that Member State.

SECTION 5
Jurisdiction over individual contracts of employment

Article 20
1. In matters relating to individual contracts of employment, jurisdiction shall be determined by this Section, without prejudice to Article 6, point 5 of Article 7 and, in the case of proceedings brought against an employer, point 1 of Article 8.
2. Where an employee enters into an individual contract of employment with an employer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, the employer shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

Article 21
1. An employer domiciled in a Member State may be sued:
(a) in the courts of the Member State in which he is domiciled; or
(b) in another Member State:
(i) in the courts for the place where or from where the employee habitually carries out his work or in the courts for the last place where he did so; or
(ii) if the employee does not or did not habitually carry out his work in any one country, in the courts for the place where the business which engaged the employee is or was situated.
2. An employer not domiciled in a Member State may be sued in a court of a Member State in accordance with point (b) of paragraph 1.

Article 22
1. An employer may bring proceedings only in the courts of the Member State in which the employee is domiciled.
2. The provisions of this Section shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 23
The provisions of this Section may be departed from only by an agreement:
(1) which is entered into after the dispute has arisen; or
(2) which allows the employee to bring proceedings in courts other than those indicated in this Section.

SECTION 6
Exclusive jurisdiction

Article 24
The following courts of a Member State shall have exclusive jurisdiction, regardless of the domicile of the parties:
(1) in proceedings which have as their object rights in rem in immovable property or tenancies of immovable property, the courts of the Member State in which the property is situated.
However, in proceedings which have as their object tenancies of immovable property concluded for temporary private use for a maximum period of six consecutive months, the courts of the Member State in which the defendant is domiciled shall also have jurisdiction, provided that the tenant is a natural person and that the landlord and the tenant are domiciled in the same Member State;
(2) in proceedings which have as their object the validity of the constitution, the nullity or the dissolution of companies or other legal persons or associations of natural or legal persons, or the validity of the decisions of their organs, the courts of the Member State in which the company, legal person or association has its seat. In order to determine that seat, the court shall apply its rules of private international law;
(3) in proceedings which have as their object the validity of entries in public registers, the courts of the Member State in which the register is kept;
(4) in proceedings concerned with the registration or validity of patents, trade marks, designs, or other similar rights required to be deposited or registered, irrespective of whether the issue is raised by way of an action or as a defence, the courts of the Member State in which the deposit or registration has been applied for, has taken place or is under the terms of an instrument of the Union or an international convention deemed to have taken place.
Without prejudice to the jurisdiction of the European Patent Office under the Convention on the Grant of European Patents, signed at Munich on 5 October 1973, the courts of each Member State shall have exclusive jurisdiction in proceedings concerned with the registration or validity of any European patent granted for that Member State;
(5) in proceedings concerned with the enforcement of judgments, the courts of the Member State in which the judgment has been or is to be enforced.

SECTION 7
Prorogation of jurisdiction

Article 25
1. If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship,
that court or those courts shall have jurisdiction, unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise. The agreement conferring jurisdiction shall be either:

(a) an instrument evidenced in writing;
(b) a form which accords with practices which the parties have established between themselves; or
(c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.

2. Any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'.

3. The court or courts of a Member State on which a trust instrument has conferred jurisdiction shall have exclusive jurisdiction in any proceedings brought against a settlor, trustee or beneficiary, if relations between those persons or their rights or obligations under the trust are involved.

4. Agreements or provisions of a trust instrument conferring jurisdiction shall have no legal force if they are contrary to Articles 15, 19 or 23, or if the courts whose jurisdiction they purport to exclude have exclusive jurisdiction by virtue of Article 24.

5. An agreement conferring jurisdiction which forms part of a contract shall be treated as an agreement independent of the other terms of the contract.

The validity of the agreement conferring jurisdiction cannot be contested solely on the ground that the contract is not valid.

Article 26

1. Apart from jurisdiction derived from other provisions of this Regulation, a court of a Member State before which a defendant enters an appearance shall have jurisdiction. This rule shall not apply where appearance was entered to contest the jurisdiction, or where another court has exclusive jurisdiction by virtue of Article 24.

2. In matters referred to in Sections 3, 4 or 5 where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee is the defendant, the court shall, before assuming jurisdiction under paragraph 1, ensure that the defendant is informed of his right to contest the jurisdiction of the court and of the consequences of entering or not entering an appearance.

SECTION 8

Examination as to jurisdiction and admissibility

Article 27

Where a court of a Member State is seised of a claim which is principally concerned with a matter over which the courts of another Member State have exclusive jurisdiction by virtue of Article 24, it shall declare of its own motion that it has no jurisdiction.

Article 28

1. Where a defendant domiciled in one Member State is sued in a court of another Member State and does not enter an appearance, the court shall declare of its own motion that it has no jurisdiction unless its jurisdiction is derived from the provisions of this Regulation.

2. The court shall stay the proceedings so long as it is not shown that the defendant has been able to receive the document instituting the proceedings or an equivalent document in sufficient time to enable him to arrange for his defence, or that all necessary steps have been taken to this end.

3. Article 19 of Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) [135] shall apply instead of paragraph 2 of this Article if the document instituting the proceedings or an equivalent document had to be transmitted from one Member State to another pursuant to that Regulation.

4. Where Regulation (EC) No 1393/2007 is not applicable, Article 15 of the Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters shall apply if the document instituting the proceedings or an equivalent document had to be transmitted abroad pursuant to that Convention.

SECTION 9

Lis pendens — related actions

Article 29

1. Without prejudice to Article 31(2), where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established.

2. In cases referred to in paragraph 1, upon request by a court seised of the dispute, any other court seised shall without delay inform the former court of the date when it was seised in accordance with Article 32.

3. Where the jurisdiction of the court first seised is established, any court other than the court first seised shall decline jurisdiction in favour of that court.

Article 30

1. Where related actions are pending in the courts of different Member States, any court other than the court first seised may stay its proceedings.

2. Where the action in the court first seised is pending at first instance, any other court may also, on the application of one of the parties, decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.

3. For the purposes of this Article, actions are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

Article 31

1. Where actions come within the exclusive jurisdiction of several courts, any court other than the court first seised shall decline jurisdiction in favour of that court.

2. Without prejudice to Article 26, where a court of a Member State on which an agreement as referred to in Article 25 confers exclusive jurisdiction is seised, any court of another Member State shall stay the proceedings until such time as the court seised on the basis of the agreement declares that it has no jurisdiction under the agreement.

3. Where the court designated in the agreement has established jurisdiction in accordance with the agreement, any court of another Member State shall decline jurisdiction in favour of that court.

4. Paragraphs 2 and 3 shall not apply to matters referred to in Sections 3, 4 or 5 where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee is the claimant and the agreement is not valid under a provision contained within those Sections.

Article 32

1. For the purposes of this Section, a court shall be deemed to be seised:

(a) at the time when the document instituting the proceedings or an equivalent document is lodged with the court, provided that the claimant has not subsequently failed to take the steps he was required to take to have service effected on the defendant; or

(b) if the document has to be served before being lodged with the court, at the time when it is received by the authority responsible for service, provided that the claimant has not subsequently failed to take the steps he was required to take to have the document lodged with the court.

The authority responsible for service referred to in point (b) shall be the first authority receiving the documents to be served.
2. The court, or the authority responsible for service, referred to in paragraph 1, shall note, respectively, the date of the lodging of the document instituting the proceedings or the equivalent document, or the date of receipt of the documents to be served.  

Article 33  
1. Where jurisdiction is based on Article 4 or on Articles 7, 8 or 9 and proceedings are pending before a court of a third State at the time when a court in a Member State is seised of an action involving the same cause of action and between the same parties as the proceedings in the court of the third State, the court of the Member State may stay the proceedings if:  
(a) it is expected that the court of the third State will give a judgment capable of recognition and, where applicable, of enforcement in that Member State; and  
(b) the court of the Member State is satisfied that a stay is necessary for the proper administration of justice.  
2. The court of the Member State may continue the proceedings at any time if:  
(a) the proceedings in the court of the third State are themselves stayed or discontinued;  
(b) it appears to the court of the Member State that the proceedings in the court of the third State are unlikely to be concluded within a reasonable time; or  
(c) the continuation of the proceedings is required for the proper administration of justice.  
3. The court of the Member State shall dismiss the proceedings if the proceedings in the court of the third State are concluded and have resulted in a judgment capable of recognition and, where applicable, of enforcement in that Member State.  
4. The court of the Member State shall apply this Article on the application of one of the parties or, where possible under national law, of its own motion.  

Article 34  
1. Where jurisdiction is based on Article 4 or on Articles 7, 8 or 9 and an action is pending before a court of a third State at the time when a court in a Member State is seised of an action which is related to the action in the court of the third State, the court of the Member State may stay the proceedings if:  
(a) it is expedient to hear and determine the related actions together to avoid the risk of irreconcilable judgments resulting from separate proceedings;  
(b) it is expected that the court of the third State will give a judgment capable of recognition and, where applicable, of enforcement in that Member State; and  
(c) the court of the Member State is satisfied that a stay is necessary for the proper administration of justice.  
2. The court of the Member State may continue the proceedings at any time if:  
(a) it appears to the court of the Member State that there is no longer a risk of irreconcilable judgments;  
(b) the proceedings in the court of the third State are themselves stayed or discontinued;  
(c) it appears to the court of the Member State that the proceedings in the court of the third State are unlikely to be concluded within a reasonable time; or  
(d) the continuation of the proceedings is required for the proper administration of justice.  
3. The court of the Member State may dismiss the proceedings if the proceedings in the court of the third State are concluded and have resulted in a judgment capable of recognition and, where applicable, of enforcement in that Member State.  
4. The court of the Member State shall apply this Article on the application of one of the parties or, where possible under national law, of its own motion.  

SECTION 10  
Provisional, including protective measures  
Article 35  
Application may be made to the courts of a Member State for such provisional, including protective, measures as may be available under the law of that Member State, even if the courts of another Member State have jurisdiction as to the substance of the matter.  

CHAPTER III  
RECOGNITION AND ENFORCEMENT  
SECTION 1  
Recognition  
Article 36  
1. A judgment given in a Member State shall be recognised in the other Member States without any special procedure being required.  
2. Any interested party may, in accordance with the procedure provided for in Subsection 2 of Section 3, apply for a decision that there are no grounds for refusal of recognition as referred to in Article 45.  
3. If the outcome of proceedings in a court of a Member State depends on the determination of an incidental question of refusal of recognition, that court shall have jurisdiction over that question.  

Article 37  
1. A party who wishes to invoke in a Member State a judgment given in another Member State shall produce:  
(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity; and  
(b) the certificate issued pursuant to Article 53.  
2. The court or authority before which a judgment given in another Member State is invoked may, where necessary, require the party invoking it to provide, in accordance with Article 57, a translation or a transliteration of the contents of the certificate referred to in point (b) of paragraph 1. The court or authority may require the party to provide a translation of the judgment instead of a translation of the contents of the certificate if it is unable to proceed without such a translation.  

Article 38  
The court or authority before which a judgment given in another Member State is invoked may suspend the proceedings, in whole or in part, if:  
(a) the judgment is challenged in the Member State of origin; or  
(b) an application has been submitted for a decision that there are no grounds for refusal of recognition as referred to in Article 45 or for a decision that the recognition is to be refused on the basis of one of those grounds.  

SECTION 2  
Enforcement  
Article 39  
A judgment given in a Member State which is enforceable in that Member State shall be enforceable in the other Member States without any declaration of enforceability being required.  

Article 40  
An enforceable judgment shall carry with it by operation of law the power to proceed to any protective measures which exist under the law of the Member State addressed.  

Article 41  
1. Subject to the provisions of this Section, the procedure for the enforcement of judgments given in another Member State shall be governed by the law of the Member State addressed. A judgment given in a Member State which is enforceable in the Member State addressed shall be enforced there under the same conditions as a judgment given in the Member State addressed.  
2. Notwithstanding paragraph 1, the grounds for refusal or of suspension of enforcement under the law of the Member State addressed shall apply in so far as they are not incompatible with the grounds referred to in Article 45.  
3. The party seeking the enforcement of a judgment given in another Member State shall not be required to have a postal address in the Member State addressed. Nor shall that party be required to have an authorised representative in the Member State addressed unless such a representative is mandatory irrespective of the nationality or the domicile of the parties.
Article 42
1. For the purposes of enforcement in a Member State of a judgment given in another Member State, the applicant shall provide the competent enforcement authority with:
(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity;
(b) the certificate issued pursuant to Article 53, certifying that the judgment is enforceable and containing an extract of the judgment as well as, where appropriate, relevant information on the recoverable costs of the proceedings and the calculation of interest; and
2. For the purposes of enforcement in a Member State of a judgment given in another Member State ordering a provisional, including a protective, measure, the applicant shall provide the competent enforcement authority with:
(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity;
(b) the certificate issued pursuant to Article 53, containing a description of the measure and certifying that:
(i) the court has jurisdiction as to the substance of the matter;
(ii) the judgment is enforceable in the Member State of origin; and
(c) where the measure was ordered without the defendant being summoned to appear, proof of service of the judgment.
3. The competent enforcement authority may, where necessary, require the applicant to provide, in accordance with Article 57, a translation or a transliteration of the contents of the certificate.
4. The competent enforcement authority may require the applicant to provide a translation of the judgment only if it is unable to proceed without such a translation.

Article 43
1. Where enforcement is sought of a judgment given in another Member State, the certificate issued pursuant to Article 53 shall be served on the person against whom the enforcement is sought prior to the first enforcement measure. The certificate shall be accompanied by the judgment, if not already served on that person.
2. Where the person against whom enforcement is sought is domiciled in a Member State other than the Member State of origin, he may request a translation of the judgment in order to contest the enforcement if the judgment is not written in or accompanied by a translation into either of the following languages:
(a) a language which he understands; or
(b) the official language of the Member State in which he is domiciled or, where there are several official languages in that Member State, the official language or one of the official languages of the place where he is domiciled.
Where a translation of the judgment is requested under the first subparagraph, no measures of enforcement may be taken other than protective measures until that translation has been provided to the person against whom enforcement is sought.
This paragraph shall not apply if the judgment has already been served on the person against whom enforcement is sought in one of the languages referred to in the first subparagraph or is accompanied by a translation into one of those languages.
3. This Article shall not apply to the enforcement of a protective measure in a judgment or where the person seeking enforcement proceeds to protective measures in accordance with Article 40.

Article 44
1. In the event of an application for refusal of enforcement of a judgment pursuant to Subsection 2 of Section 3, the court in the Member State addressed may, on the application of the person against whom enforcement is sought:
(a) limit the enforcement proceedings to protective measures;
(b) make enforcement conditional on the provision of such security as it shall determine; or
(c) suspend, either wholly or in part, the enforcement proceedings.
2. The competent authority in the Member State addressed shall, on the application of the person against whom enforcement is sought, suspend the enforcement proceedings where the enforceability of the judgment is suspended in the Member State of origin.

SECTION 3
Refusal of recognition and enforcement

Subsection 1
Refusal of recognition

Article 45
1. On the application of any interested party, the recognition of a judgment shall be refused:
(a) if such recognition is manifestly contrary to public policy (ordre public) in the Member State addressed;
(b) where the judgment was given in default of appearance, if the defendant was not served with the document which instituted the proceedings or with an equivalent document in sufficient time and in such a way as to enable him to arrange for his defence, unless the defendant failed to commence proceedings to challenge the judgment when it was possible for him to do so;
(c) if the judgment is irreconcilable with a judgment given between the same parties in the Member State addressed;
(d) if the judgment is irreconcilable with an earlier judgment given in another Member State or in a third State involving the same cause of action and between the same parties, provided that the earlier judgment fulfils the conditions necessary for its recognition in the Member State addressed; or
(e) if the judgment conflicts with:
(i) Sections 3, 4 or 5 of Chapter II where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee was the defendant; or
(ii) Section 6 of Chapter II.
2. In its examination of the grounds of jurisdiction referred to in point (e) of paragraph 1, the court to which the application was submitted shall be bound by the findings of fact on which the court of origin based its jurisdiction.
3. Without prejudice to point (e) of paragraph 1, the jurisdiction of the court of origin may not be reviewed. The test of public policy referred to in point (a) of paragraph 1 may not be applied to the rules relating to jurisdiction.
4. The application for refusal of recognition shall be made in accordance with the procedures provided for in Subsection 2 and, where appropriate, Section 4.

Subsection 2
Refusal of enforcement

Article 46
On the application of the person against whom enforcement is sought, the enforcement of a judgment shall be refused where one of the grounds referred to in Article 45 is found to exist.

Article 47
1. The application for refusal of enforcement shall be submitted to the court which the Member State concerned has communicated to the Commission pursuant to point (a) of Article 75 as the court to which the application is to be submitted.
2. The procedure for refusal of enforcement shall be so far as it is not covered by this Regulation, be governed by the law of the Member State addressed.
3. The applicant shall provide the court with a copy of the judgment and, where necessary, a translation or transliteration of it. The court may dispense with the production of the documents referred to in the first subparagraph if it already possesses them or if it considers it unreasonable to require the applicant to provide them. In the latter case, the court may require the other party to provide those documents.
4. The party seeking the refusal of enforcement of a judgment given in another Member State shall not be
required to have a postal address in the Member State addressed. Nor shall that party be required to have an authorised representative in the Member State addressed unless such a representative is mandatory irrespective of the nationality or the domicile of the parties.

Article 48
The court shall decide on the application for refusal of enforcement without delay.

Article 49
1. The decision on the application for refusal of enforcement may be appealed against by either party.
2. The appeal is to be lodged with the court which the Member State concerned has communicated to the Commission pursuant to point (b) of Article 75 as the court with which such an appeal is to be lodged.

Article 50
1. The court to which an application for refusal of enforcement is submitted or the court which hears an appeal lodged under Article 49 or Article 50 may stay the proceedings if an ordinary appeal has been lodged against the judgment in the Member State of origin or if the time for such an appeal has not yet expired. In the latter case, the court may specify the time within which such an appeal is to be lodged.
2. Where the judgment was given in Ireland, Cyprus or the United Kingdom, any form of appeal available in the Member State of origin shall be treated as an ordinary appeal for the purposes of paragraph 1.

SECTION 4
Common provisions
Article 51
Under no circumstances may a judgment given in a Member State be reviewed as to its substance in the Member State addressed.

Article 52
The court of origin shall, at the request of any interested party, issue the certificate using the form set out in Annex I.

Article 53
1. If a judgment contains a measure or an order which is not known in the law of the Member State addressed, that measure or order shall, to the extent possible, be adapted to a measure or an order known in the law of that Member State which has equivalent effects attached to it and which pursues similar aims and interests.
2. Any party may challenge the adaptation of the measure or order before a court.
3. If necessary, the party invoking the judgment or seeking its enforcement may be required to provide a translation or a transliteration of the judgment.

Article 54
A judgment given in a Member State which orders a payment by way of a penalty shall be enforceable in the Member State addressed only if the amount of the payment has been finally determined by the court of origin.

Article 55
No security, bond or deposit, however described, shall be required of a party who in one Member State applies for the enforcement of a judgment given in another Member State on the ground that he is a foreign national or that he is not domiciled or resident in the Member State addressed.

Article 56
1. When a translation or a transliteration is required under this Regulation, such translation or transliteration shall be into the official language of the Member State concerned or, where there are several official languages in that Member State, into the official language or one of the official languages of court proceedings of the place where a judgment given in another Member State is invoked.
2. For the purposes of the forms referred to in Articles 53 and 60, translations or transliterations may also be into any other official language or languages of the institutions of the Union that the Member State concerned has indicated it can accept.
3. Any translation made under this Regulation shall be done by a person qualified to do translations in one of the Member States.

CHAPTER IV
AUTHENTIC INSTRUMENTS AND COURT SETTLEMENTS
Article 58
1. An authentic instrument which is enforceable in the Member State of origin shall be enforceable in the other Member States without any declaration of enforceability being required. Enforcement of the authentic instrument may be refused only if such enforcement is manifestly contrary to public policy (ordre public) in the Member State addressed.

Article 59
A court settlement which is enforceable in the Member State of origin shall be enforced in the other Member States under the same conditions as authentic instruments.

Article 60
The competent authority or court of the Member State of origin shall, at the request of any interested party, issue the certificate using the form set out in Annex II containing a summary of the enforceable obligation recorded in the authentic instrument or of the agreement between the parties recorded in the court settlement.

CHAPTER V
GENERAL PROVISIONS
Article 61
No legalisation or other similar formality shall be required for documents issued in a Member State in the context of this Regulation.

Article 62
1. In order to determine whether a party is domiciled in the Member State whose courts are seised of a matter, the court shall apply its internal law.
2. If a party is not domiciled in the Member State whose courts are seised of the matter, then, in order to determine whether the party is domiciled in another Member State, the court shall apply the law of that Member State.

Article 63
1. For the purposes of this Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its:
(a) statutory seat;
(b) central administration; or
(c) principal place of business.
2. For the purposes of Ireland, Cyprus and the United Kingdom, ‘statutory seat’ means the registered office or, where there is no such office anywhere, the place of incorporation or, where there is no such place anywhere, the place under the law of which the formation took place.
3. In order to determine whether a trust is domiciled in the Member State whose courts are seised of the matter, the court shall apply its rules of private international law.

Article 64
Without prejudice to any more favourable provisions of national laws, persons domiciled in a Member State who are being prosecuted in the criminal courts of another Member State of which they are not nationals for an offence which was not intentionally committed may be defended by
persons qualified to do so, even if they do not appear in person. However, the court seised of the matter may order appearance in person; in the case of failure to appear, a judgment given in the civil action without the person concerned having had the opportunity to arrange for his defence need not be recognised or enforced in the other Member States.

**Article 65**
1. The jurisdiction specified in point 2 of Article 8 and Article 13 in actions on a warranty or guarantee or in any other third-party proceedings may be resorted to in the Member States included in the list established by the Commission pursuant to point (b) of Article 76(1) and Article 76(2) only in so far as permitted under national law. A person domiciled in another Member State may be invited to join the proceedings before the courts of those Member States pursuant to the rules on third-party notice referred to in that list.
2. Judgments given in a Member State by virtue of point 2 of Article 8 or Article 13 shall be recognised and enforced in accordance with Chapter III in any other Member State. Any effects which judgments given in the Member States included in the list referred to in paragraph 1 may have, in accordance with the law of those Member States, on third parties by application of paragraph 1 shall be recognised in all Member States.
3. The Member States included in the list referred to in paragraph 1 shall, within the framework of the European Judicial Network in civil and commercial matters established by Council Decision 2001/470/EC ('the European Judicial Network') provide information on how to determine, in accordance with their national law, the effects of the judgments referred to in the second sentence of paragraph 2.

**CHAPTER VI**

**TRANSITIONAL PROVISIONS**

**Article 66**
1. This Regulation shall apply only to legal proceedings instituted, to authentic instruments formally drawn up or registered and to court settlements approved or concluded on or after 10 January 2015.
2. Notwithstanding Article 80, Regulation (EC) No 44/2001 shall continue to apply to judgments given in legal proceedings instituted, to authentic instruments formally drawn up or registered and to court settlements approved or concluded before 10 January 2015 which fall within the scope of that Regulation.

**CHAPTER VII**

**RELATIONSHIP WITH OTHER INSTRUMENTS**

**Article 67**
This Regulation shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union or in national legislation harmonised pursuant to such instruments.

**Article 68**
1. This Regulation shall, as between the Member States, supersede the 1968 Brussels Convention, except as regards the territories of the Member States which fall within the territorial scope of that Convention and which are excluded from this Regulation pursuant to Article 355 of the TFEU.
2. In so far as this Regulation replaces the provisions of the 1968 Brussels Convention between the Member States, any reference to that Convention shall be understood as a reference to this Regulation.

**Article 69**
Subject to Articles 70 and 71, this Regulation shall, as between the Member States, supersede the conventions that cover the same matters as those to which this Regulation applies. In particular, the conventions included in the list established by the Commission pursuant to point (c) of Article 76(1) and Article 76(2) shall be superseded.

**Article 70**
1. The conventions referred to in Article 69 shall continue to have effect in relation to matters to which this Regulation does not apply.
2. They shall continue to have effect in respect of judgments given, authentic instruments formally drawn up or registered and court settlements approved or concluded before the date of entry into force of Regulation (EC) No 44/2001.

**Article 71**
1. This Regulation shall not affect any conventions to which the Member States are parties and which, in relation to particular matters, govern jurisdiction or the recognition or enforcement of judgments.
2. With a view to its uniform interpretation, paragraph 1 shall be applied in the following manner:
(a) this Regulation shall not prevent a court of a Member State which is party to a convention on a particular matter from assuming jurisdiction in accordance with that convention, even where the defendant is domiciled in another Member State which is not party to that convention. The court hearing the action shall, in any event, apply Article 28 of this Regulation;
(b) judgments given in a Member State by a court in the exercise of jurisdiction provided for in a convention on a particular matter shall be recognised and enforced in the other Member States in accordance with this Regulation.

Where a convention on a particular matter to which both the Member States of origin and the Member State addressed are parties lays down conditions for the recognition or enforcement of judgments, those conditions shall apply. In any event, the provisions of this Regulation on recognition and enforcement of judgments may be applied.

**Article 72**
This Regulation shall not affect agreements by which Member States, prior to the entry into force of Regulation (EC) No 44/2001, undertook pursuant to Article 59 of the 1968 Brussels Convention not to recognise judgments given, in particular in other Contracting States to that Convention, against defendants domiciled or habitually resident in a third State where, in cases provided for in Article 4 of that Convention, the judgment could only be founded on a ground of jurisdiction specified in the second paragraph of Article 3 of that Convention.

**Article 73**
1. This Regulation shall not affect the application of the 2007 Lugano Convention.
2. This Regulation shall not affect the application of the 1958 New York Convention.
3. This Regulation shall not affect the application of bilateral conventions and agreements between a third State and a Member State concluded before the date of entry into force of Regulation (EC) No 44/2001 which concern matters governed by this Regulation.

**CHAPTER VIII**

**FINAL PROVISIONS**

**Article 74**
The Member States shall provide, within the framework of the European Judicial Network and with a view to making the information available to the public, a description of national rules and procedures concerning enforcement, including authorities competent for enforcement, and information on any limitations on enforcement, in particular debtor protection rules and limitation or prescription periods.

The Member States shall keep this information permanently updated.

**Article 75**
By 10 January 2014, the Member States shall communicate to the Commission:
(a) the courts to which the application for refusal of enforcement is to be submitted pursuant to Article 47(1);
(b) the courts with which an appeal against the decision on the application for refusal of enforcement is to be lodged pursuant to Article 49(2).
[c]he courts with which any further appeal is to be lodged pursuant to Article 50; and

(d) the languages accepted for translations of the forms as referred to in Article 57(2).

The Commission shall make the information publicly available through any appropriate means, in particular through the European Judicial Network.

Article 76
1. The Member States shall notify the Commission of:
   (a) the rules of jurisdiction referred to in Articles 5(2) and 6(2);
   (b) the rules on third-party notice referred to in Article 65; and
   (c) the conventions referred to in Article 69.
2. The Commission shall, on the basis of the notifications by the Member States referred to in paragraph 1, establish the corresponding lists.
3. The Member States shall notify the Commission of any subsequent amendments required to be made to those lists. The Commission shall amend those lists accordingly.
4. The Commission shall publish the lists and any subsequent amendments made to them in the Official Journal of the European Union.

Article 77
The Commission shall be empowered to adopt delegated acts in accordance with Article 78 concerning the amendment of Annexes I and II.

Article 78
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 77 shall be conferred on the Commission for an indeterminate period of time from 9 January 2013.
3. The delegation of power referred to in Article 77 may be revoked at any time by the European Parliament or by the Council.
4. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Article 79
By 11 January 2022 the Commission shall present a report to the European Parliament, to the Council and to the European Economic and Social Committee on the application of this Regulation. That report shall include an evaluation of the possible need for a further extension of the rules on jurisdiction to defendants not domiciled in a Member State, taking into account the operation of this Regulation and possible developments at international level. Where appropriate, the report shall be accompanied by a proposal for amendment of this Regulation.

Article 80
This Regulation shall repeal Regulation (EC) No 44/2001. References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table set out in Annex III.

Article 81
This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 10 January 2015, with the exception of Articles 75 and 76, which shall apply from 10 January 2014. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 12 December 2012.

For the European Parliament
The President
M. SCHULZ
For the Council
The President
A. D. MAVROYIANNIS
Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

Whereas:

(1) The Community has set itself the objective of maintaining and developing an area of freedom, security and justice. For the progressive establishment of such an area, the Community is to adopt measures relating to judicial cooperation in civil matters with a cross-border impact to the extent necessary for the proper functioning of the internal market.

(2) According to Article 65, point (b) of the Treaty, these measures are to include those promoting the compatibility of the rules applicable in the Member States concerning the conflict of laws and of jurisdiction.

(3) The European Council meeting in Tampere on 15 and 16 October 1999 endorsed the principle of mutual recognition of judgments and other decisions of judicial authorities as the cornerstone of judicial cooperation in civil matters and invited the Council and the Commission to adopt a programme of measures to implement that principle.

(4) On 30 November 2000 the Council adopted a joint Commission and Council programme of measures for implementation of the principle of mutual recognition of decisions in civil and commercial matters (3). The programme identifies measures relating to the harmonisation of conflict-of-law rules as those facilitating the mutual recognition of judgments.

(5) The programme (4), adopted by the European Council on 5 November 2004, called for work to be pursued actively on the conflict-of-law rules regarding contractual obligations (Rome I).

(6) The proper functioning of the internal market creates a need, in order to improve the predictability of the outcome of litigation, certainty as to the law applicable and the free movement of judgments, for the conflict-of-law rules in the Member States to designate the same national law irrespective of the country of the court in which an action is brought.


(8) Family relationships should cover parentage, marriage, affinity and collateral relatives. The reference in Article 1(2) to relationships having comparable effects to marriage and other family relationships should be interpreted in accordance with the law of the Member State in which the court is seised.

(9) Obligations under bills of exchange, cheques and promissory notes and other negotiable instruments should also cover bills of lading to the extent that the obligations under the bill of lading arise out of its negotiable character.

(10) Obligations arising out of dealings prior to the conclusion of the contract are covered by Article 12 of Regulation (EC) No 864/2007. Such obligations should therefore be excluded from the scope of this Regulation.

(11) The parties’ freedom to choose the applicable law should be one of the cornerstones of the system of conflict-of-law rules in matters of contractual obligations.

(12) An agreement between the parties to confer on one or more courts or tribunals of a Member State exclusive jurisdiction to determine disputes under the contract should be one of the factors to be taken into account in determining whether a choice of law has been clearly demonstrated.

(13) This Regulation does not preclude parties from incorporating by reference into their contract a non-State body of law or an international convention.

(14) Should the Community adopt, in an appropriate legal instrument, rules of substantive contract law, including standard terms and conditions, such instrument may provide that the parties may choose to apply those rules.

(15) Where a choice of law is made and all other elements relevant to the situation are located in a country other than the country whose law has been chosen, the choice of law should not prejudice the application of provisions of the law of that country which cannot be derogated from by agreement. This rule should apply whether or not the choice of law was accompanied by a choice of court or tribunal. Where no substantial change is intended as compared with Article 5(3) of the 1980 Convention on the Law Applicable to Contractual Obligations (7) (the Rome Convention), the wording of this Regulation is aligned as far as possible with Article 14 of Regulation (EC) No 864/2007.

(16) To contribute to the general objective of this Regulation, legal certainty in the European judicial area, the conflict-of-law rules should be highly foreseeable. The courts should, however, retain a degree of discretion to determine the law that is most closely connected to the situation.

(17) As far as the applicable law in the absence of choice is concerned, the concept of ‘provision of services’ and ‘sale of goods’ should be interpreted in the same way as when applying Article 5 of Regulation (EC) No 44/2001. In so far as goods and provision of services are covered by that Regulation, although franchise and distribution contracts are contracts for services, they are the subject of specific rules.

(18) As far as the applicable law in the absence of choice is concerned, multilateral systems should not be regarded as facilitating the free movement of judgments, in which trading is conducted, such as regulated markets and multilateral trading facilities as referred to in Article 4 of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (8), regardless of whether or not they rely on a central counterparty.

(19) Where there has been no choice of law, the applicable law should be determined in accordance with the rule specified for the particular type of contract. Where the contract cannot be categorised as being one of the specified types or where its elements fall within more than one of the specified types, it should be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence. In the case of a contract consisting of a bundle of rights and obligations capable of being categorised as falling within more than one of the specified types, it should be governed by the law of the country which cannot be derogated from by the country whose law has been chosen, the choice of law should therefore be excluded from the scope of this Regulation.

(20) Where the contract is manifestly more closely connected with a country other than that indicated in Article 4(1) or (2), an escape clause should provide that the law of that other country is to apply. In order to determine that the country, account should be taken, inter alia, of whether the contract in question has a very close relationship with another contract or contracts.

(21) In the absence of choice, where the applicable law cannot be determined either on the basis of the fact that the contract can be categorised as one of the specified types or as being the law of the country of habitual residence of the party required to effect the characteristic performance of the contract, the contract should be governed by the law of the country with which it is most closely connected. In order to determine that a country, account should be taken, inter alia, of whether the contract in question has a very close relationship with another contract or contracts.

(22) As regards the interpretation of contracts for the carriage of goods, no change in substance is intended with respect to Article 4(3), third sentence, of the Rome Convention. Consequently, single-voyage charter parties and other contracts the main purpose of which is the carriage of goods should be treated as contracts for the carriage of goods. For the purposes of this Regulation, the term ‘consignor’ should refer to any person who enters into a contract of carriage with the carrier and the term ‘the carrier’ should refer to the party to the contract who
undertakes to carry the goods, whether or not he performs the carriage himself.

(23) As regards contracts concluded with parties regarded as being weaker, those parties should be protected by conflict-of-law rules that are more favourable to their interests than the general rules.

(24) With more specific reference to consumer contracts, the conflict-of-law rule should make it possible to cut the cost of settling disputes concerning what are commonly relatively small claims and to take account of the development of distance selling techniques. Consistency with Regulation (EC) No 44/2001 requires both that there be a reference to the concept of directed activity as a condition for applying the consumer protection rule and that the concept be interpreted harmoniously in Regulation (EC) No 44/2001 and this Regulation, bearing in mind that a joint declaration by the Council and the Commission on Article 15 of Regulation (EC) No 44/2001 states that ‘for Article 15(1)(c) to be applicable it is not sufficient for an undertaking to target its activities at the Member State of the consumer’s residence, or at a number of Member States including that Member State, a contract must also be concluded within the framework of its activities’. The declaration also states that ‘the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. In this respect, the language or currency which a website uses does not constitute a relevant factor’.

(25) Consumers should be protected by such rules of the country of their habitual residence that cannot be derogated from by agreement, provided that the consumer contract has been concluded as a result of the professional pursuing his commercial or professional activities in that particular country. The same protection should be guaranteed if the professional, while not pursuing his commercial or professional activities in the country where the consumer has his habitual residence, directs his activities by any means to that country or to several countries, including that country, and the contract is concluded as a result of such activities.

(26) For the purposes of this Regulation, financial services such as investment services and activities and ancillary services provided by a professional to a consumer, as referred to in sections A and B of Annex I to Directive 2004/39/EC, and contracts for the sale of units in collective investment undertakings, whether or not covered by Council Directive 85/611/EEC of 20 December 1985 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (9), should be subject to Article 6 of this Regulation. Consequently, when a reference is made to terms and conditions governing the issuance or offer to the public of transferable securities or to the subscription and redemption of units in collective investment undertakings, that reference should include all aspects binding the issuer or the offeror to the consumer, but should not include those aspects involving the provision of financial services.

(27) Various exceptions should be made to the general conflict-of-law rule for consumer contracts. Under one such exception the general rule should not apply to contracts relating to rights in rem in immovable property or tenancies of such property unless the contract relates to the right to use immovable property on a timeshare basis within the meaning of Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of the right to use immovable properties on a timeshare basis (10).

(28) It is important to ensure that rights and obligations which constitute a financial instrument are not covered by the general rule applicable to consumer contracts, as that could lead to different laws being applicable to each of the instruments issued, therefore changing their nature and preventing their fungible trading and offering. Likewise, whenever such instruments are issued or offered, the contractual relationship established between the issuer or the offeror and the consumer should not necessarily be subject to the mandatory application of the law of the country of habitual residence of the consumer, as there is a need to ensure uniformity in the terms and conditions of an issuance or an offer. The same rationale should apply with regard to multi-legal systems covered by Regulation (EC) No 44/2001, in respect of which it should be ensured that the law of the country of habitual residence of the consumer will not interfere with the rules applicable to contracts concluded within those systems or with the operator of such systems.

(29) For the purposes of this Regulation, references to rights and obligations relating to the terms and conditions governing the issuance, offers to the public or public take-over bids of transferable securities and references to the subscription and redemption of units in collective investment undertakings should include the terms and conditions of insurance contracts, specific provisions should ensure an adequate level of protection of passengers and policy holders. Therefore, Article 6 should not apply in the context of those particular contracts.

(30) Where an insurance contract not covering a large risk covers more than one risk, at least one of which is situated in a Member State and at least one of which is situated in a third country, the special rules on insurance contracts in this Regulation should apply only to the risk or risks situated in the relevant Member State or Member States.


(32) Owing to the particular nature of contracts of carriage and insurance contracts, specific provisions should ensure an adequate level of protection of passengers and policy holders. Therefore, Article 6 should not apply in the context of those particular contracts.

(33) Where an insurance contract not covering a large risk covers more than one risk, at least one of which is situated in a Member State and at least one of which is situated in a third country, the special rules on insurance contracts in this Regulation should apply only to the risk or risks situated in the relevant Member State or Member States.

(34) The rule on individual employment contracts should not prejudice the application of the overriding mandatory provisions of the country to which a worker is posted in accordance with Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services (12).

(35) Employees should not be deprived of the protection afforded to them by provisions which cannot be derogated from by agreement or which can only be derogated from to their benefit.

(36) As regards individual employment contracts, work carried out in another country should be regarded as temporary if the employee is expected to resume working in the country of origin after carrying out his tasks abroad. The conclusion of a new contract of employment with the original employer or an employer belonging to the same group of companies as the original employer should not preclude the employee from being regarded as carrying out his work in another country temporarily.

(37) Consideration of public interest justifying the courts of the Member States the possibility, in exceptional circumstances, of applying exceptions based on public policy and overriding mandatory provisions. The concept of ‘overriding mandatory provisions’ should be distinguished from the expression ‘provisions which cannot be derogated
from by agreement’ and should be construed more restrictively.

(38) In the context of voluntary assignment, the term ‘relationship’ should make it clear that Article 14(1) also applies to the property aspects of an assignment, as between assignor and assignee. In legal orders where such aspects are treated separately from the aspects under the law of obligations. However, the term ‘relationship’ should not be understood as relating to any relationship that may exist between assignor and assignee. In particular, it should not cover preliminary questions as regards a voluntary assignment or a contractual subrogation. The term should be strictly limited to the aspects which are directly relevant to the voluntary assignment or contractual subrogation in question.

(39) For the sake of legal certainty there should be a clear definition of habitual residence, in particular for companies and other bodies, corporate or unincorporated. Unlike Article 60(1) of Regulation (EC) No 44/2001, which establishes three criteria, the conflict-of-law rule should proceed on the basis of a single criterion; otherwise, the parties would be unable to foresee the law applicable to their situation.

(40) A situation where conflict-of-law rules are dispersed among several instruments and where there are differences between those rules should be avoided. This Regulation, however, should not exclude the possibility of inclusion of conflict-of-law rules relating to contractual obligations in provisions of Community law with regard to particular matters. This Regulation should not prejudice the application of other instruments laying down provisions designed to contribute to the proper functioning of the internal market in so far as they cannot be applied in conjunction with the law designated by the rules of this Regulation. The application of provisions of the applicable law designated by the rules of this Regulation should not restrict the free movement of goods and services as regulated by Community instruments, such as Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (13).

(41) Respect for international commitments entered into by the Member States means that this Regulation should not affect international conventions to which one or more Member States are parties at the time when this Regulation is adopted. To make the rules more accessible, the Commission should publish the list of the relevant conventions in the Official Journal of the European Union on the basis of information supplied by the Member States.

(42) The Commission will make a proposal to the European Parliament and to the Council concerning the procedures and conditions according to which Member States would be entitled to negotiate and conclude, on their own behalf, agreements with third countries in individual and exceptional cases concerning sectoral matters and containing provisions on the applicable law to cover preliminary questions involving the status or legal capacity of natural persons, or without prejudice to Article 13;

(43) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can therefore be achieved only by reason of the scale and effects of this Regulation, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to attain its objective.

(44) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Ireland has notified its wish to take part in the adoption and application of the present Regulation.

(45) In accordance with Articles 1 and 2 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community, and without prejudice to Article 4 of the said Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(46) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SCOPE

Article 1

Material scope

1. This Regulation shall apply, in situations involving a conflict of laws, to contractual obligations in civil and commercial matters.

It shall not apply, in particular, to revenue, customs or administrative matters.

2. The following shall be excluded from the scope of this Regulation:

(a) questions involving the status or legal capacity of natural persons, without prejudice to Article 13;

(b) obligations arising out of family relationships and relationships deemed by the law applicable to such relationships to have comparable effects, including maintenance obligations;

(c) obligations arising out of matrimonial property regimes, property regimes of relationships deemed by the law applicable to such relationships to have comparable effects to marriage, and wills and succession;

(d) obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character;

(e) arbitration agreements and agreements on the choice of court;

(f) questions governed by the law of companies and other bodies, corporate or unincorporated, such as the creation, by registration or otherwise, legal capacity, internal organisation or winding-up of companies and other bodies, corporate or unincorporated, and the personal liability of officers and members as such for the obligations of the company or body;

(g) the question whether an agent is able to bind a principal, or an organ to bind a company or other body corporate or unincorporated, in relation to a third party;

(h) the constitution of trusts and the relationship between settlors, trustees and beneficiaries;

(i) obligations arising out of dealings prior to the conclusion of a contract;

(j) insurance contracts arising out of operations carried out by organisations other than undertakings referred to in Article 2 of Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance (14) the object of which is to provide benefits for employed or self-employed persons belonging to an undertaking or group of undertakings, or to a trade or group of trades, in the event of death or survival or of discontinuance or curtailment of activity, or of sickness related to work or accidents at work.

3. This Regulation shall not apply to evidence and procedure, without prejudice to Article 18.

4. In this Regulation, the term ‘Member State’ shall mean Member States to which this Regulation applies. However, in
Article 3(4) and Article 7 the term shall mean all the Member States.

Article 2

Universal application

Any law specified by this Regulation shall be applied whether or not it is the law of a Member State.

CHAPTER II

UNIFORM RULES

Article 3

Freedom of choice

1. A contract shall be governed by the law chosen by the parties. The choice shall be made expressly or clearly demonstrated by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or to part only of the contract.

2. The parties may at any time agree to subject the contract to a law other than that which previously governed it, whether as a result of an earlier choice made under this Article or of other provisions of this Regulation. Any change in the law to be applied that is made after the conclusion of the contract shall not prejudice its formal validity under Article 11 or adversely affect the rights of third parties.

3. Where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement.

4. Where all other elements relevant to the situation at the time of the choice are located in one or more Member States, the parties' choice of applicable law other than that of a Member State shall not prejudice the application of provisions of Community law, where appropriate as implemented in the Member State of the forum, which cannot be derogated from by agreement.

5. The existence and validity of the consent of the parties as to the choice of the applicable law shall be determined in accordance with the provisions of Articles 10, 11 and 13.

Article 4

Applicable law in the absence of choice

1. To the extent that the law applicable to the contract has not been chosen in accordance with Article 3 and without prejudice to Articles 5 to 8, the law governing the contract shall be determined as follows:

(a) a contract for the sale of goods shall be governed by the law of the country where the seller has his habitual residence;

(b) a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence;

(c) a contract relating to a right in rem in immovable property or to a tenancy of immovable property shall be governed by the law of the country where the property is situated;

(d) notwithstanding point (c), a tenancy of immovable property concluded for temporary private use for a period of no more than six consecutive months shall be governed by the law of the country where the landlord has his habitual residence, provided that the tenant is a natural person and has his habitual residence in the same country;

(e) a franchise contract shall be governed by the law of the country where the franchisee has his habitual residence;

(f) a distribution contract shall be governed by the law of the country where the distributor has his habitual residence;

(g) a contract for the sale of goods by auction shall be governed by the law of the country where the auction takes place, if such a place can be determined;

(h) a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law.

2. Where the contract is not covered by paragraph 1 or where the elements of the contract would be covered by more than one of points (a) to (h) of paragraph 1, the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence.

3. Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.

4. Where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected.

Article 5

Contracts of carriage

1. To the extent that the law applicable to a contract for the carriage of goods has not been chosen in accordance with Article 3, the law applicable shall be the law of the country of habitual residence of the carrier, provided that the place of receipt or the place of delivery or the habitual residence of the consignor is also situated in that country. If those requirements are not met, the law of the country where the place of delivery as agreed by the parties is situated shall apply.

2. To the extent that the law applicable to a contract for the carriage of passengers has not been chosen by the parties in accordance with the second subparagraph, the law applicable shall be the law of the country where the passenger has his habitual residence, provided that either the place of departure or the place of destination is situated in that country. If these requirements are not met, the law of the country where the carrier has his habitual residence shall apply.

The parties may choose as the law applicable to a contract for the carriage of passengers in accordance with Article 3 only the law of the country where:

(a) the passenger has his habitual residence; or

(b) the carrier has his habitual residence; or

(c) the carrier has his place of central administration; or

(d) the place of departure is situated; or

(e) the place of destination is situated.

3. Where it is clear from all the circumstances of the case that the contract, in the absence of a choice of law, is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.

Article 6

Consumer contracts

1. Without prejudice to Articles 5 and 7, a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the consumer) with another person acting in the exercise of his trade or profession (the professional) shall be governed by
the law of the country where the consumer has his habitual residence, provided that the professional:
(a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or
(b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities.
2. Notwithstanding paragraph 1, the parties may choose the law applicable to a contract which fulfills the requirements of paragraph 1, in accordance with Article 3. Such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable on the basis of paragraph 1.
3. If the requirements in points (a) or (b) of paragraph 1 are not fulfilled, the law applicable to a contract between a consumer and a professional shall be determined pursuant to Articles 3 and 4.

4. Paragraphs 1 and 2 shall not apply to:
(a) a contract for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence;
(b) a contract of carriage other than a contract relating to package travel within the meaning of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours (15);
(c) a contract relating to a right in rem in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 94/47/EC;
(d) rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the insurance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units of collective investment undertakings in so far as these activities do not constitute provision of a financial service;
(e) a contract concluded within the type of system falling within the scope of Article 4(1)(b).

Article 7 Insurance contracts

1. This Article shall apply to contracts referred to in paragraph 2, whether or not the risk covered is situated in a Member State, and to all other insurance contracts covering risks situated inside the territory of the Member States. It shall not apply to reinsurance contracts.
2. An insurance contract covering a large risk as defined in Article 5(d) of the First Council Directive 73/239/EEC of 24 July 1973 on the coordination of laws, regulations and administrative provisions relating to the taking-up and pursuit of the business of direct insurance other than life assurance (16) shall be governed by the law chosen by the parties in accordance with Article 3 of this Regulation.
To the extent that the applicable law has not been chosen by the parties, the insurance contract shall be governed by the law of the country where the insurer has his habitual residence. Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with another country, the law of that other country shall apply.
3. In the case of an insurance contract other than a contract falling within paragraph 2, only the following laws may be chosen by the parties in accordance with Article 3:
(a) the law of any Member State where the risk is situated at the time of conclusion of the contract;
(b) the law of the country where the policy holder has his habitual residence;
(c) in the case of life assurance, the law of the Member State of which the policy holder is a national;
(d) for insurance contracts covering risks limited to events occurring in one Member State other than the Member State where the risk is situated, the law of that Member State;
(e) where the policy holder of a contract falling under this paragraph pursues a commercial or industrial activity or a liberal profession and the insurance contract covers two or more risks which relate to those activities and are situated in different Member States, the law of any of the Member States concerned or the law of the country of habitual residence of the policy holder.
Where, in the cases set out in points (a), (b) or (e), the Member States referred to grant greater freedom of choice of the law applicable to the insurance contract, the parties may take advantage of that freedom.
To the extent that the law applicable has not been chosen by the parties in accordance with this paragraph, such a contract shall be governed by the law of the Member State in which the risk is situated at the time of conclusion of the contract.
4. The following additional rules shall apply to insurance contracts covering risks for which a Member State imposes an obligation to take out insurance:
(a) the insurance contract shall not satisfy the obligation to take out insurance unless it complies with the specific provisions relating to that insurance laid down by the Member State that imposes the obligation. Where the law of the Member State in which the risk is situated and the law of the Member State imposing the obligation to take out insurance contradict each other, the latter shall prevail;
(b) by way of derogation from paragraphs 2 and 3, a Member State may lay down that the insurance contract shall be governed by the law of the Member State that imposes the obligation to take out insurance.
5. For the purposes of paragraph 3, third subparagraph, and paragraph 4, where the contract covers risks situated in more than one Member State, the contract shall be considered as constituting several contracts each relating to only one Member State.
6. For the purposes of this Article, the country in which the risk is situated shall be determined in accordance with Article 2(d) of the Second Council Directive 88/357/EEC of 22 June 1988 on the coordination of laws, regulations and administrative provisions relating to direct insurance other than life assurance and laying down provisions to facilitate the effective exercise of freedom to provide services (17) and, in the case of life assurance, the country in which the risk is situated shall be the country of the commitment within the meaning of Article 1(1)(a) of Directive 2002/83/EC.

Article 8 Individual employment contracts

1. An individual employment contract shall be governed by the law chosen by the parties in accordance with Article 3. Such a choice of law may not, however, have the result of depriving the employee of the protection afforded to him by provisions that cannot be derogated from by agreement under the law that, in the absence of choice, would have been applicable pursuant to paragraphs 2, 3 and 4 of this Article.
2. To the extent that the law applicable to the individual employment contract has not been chosen by the parties, the
such contracts shall be governed by the law of the country where the consumer has his habitual residence.
5. Notwithstanding paragraphs 1 to 4, a contract the subject matter of which is a right in rem in immovable property or a tenancy of immovable property shall be subject to the requirements of form of the law of the country where the property is situated if by that law:
(a) those requirements are imposed irrespective of the country where the contract is concluded and irrespective of the law governing the contract; and
(b) those requirements cannot be derogated from by agreement.

Article 12
Scope of the law applicable

1. The law applicable to a contract by virtue of this Regulation shall govern in particular:
(a) interpretation;
(b) performance;
(c) within the limits of the powers conferred on the court by its procedural law, the consequences of a total or partial breach of obligations, including the assessment of damages in so far as it is governed by rules of law;
(d) the various ways of extinguishing obligations, and prescription and limitation of actions;
(e) the consequences of nullity of the contract.
2. In relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall be had to the law of the country in which performance takes place.

Article 13
Incapacity

In a contract concluded between persons who are in the same country, a natural person who would have capacity under the law of that country may invoke his incapacity resulting from the law of another country, only if the other party to the contract was aware of that incapacity at the time of the conclusion of the contract or was not aware thereof as a result of negligence.

Article 14
Voluntary assignment and contractual subrogation

1. The relationship between assignor and assignee under a voluntary assignment or contractual subrogation of a claim against another person (the debtor) shall be governed by the law that applies to the contract between the assignor and assignee under this Regulation.
2. The law governing the assigned or subrogated claim shall determine its assignability, the relationship between the assignee and the debtor, the conditions under which the assignment or subrogation can be invoked against the debtor and whether the debtor’s obligations have been discharged.
3. The concept of assignment in this Article includes outright transfers of claims, transfers of claims by way of security and pledges or other security rights over claims.

Article 15
Legal subrogation

Where a person (the creditor) has a contractual claim against another (the debtor) and a third person has a duty to satisfy the creditor, or has in fact satisfied the creditor in discharge of that duty, the law which governs the third person’s duty to satisfy the creditor shall determine whether and to what
Article 16
Multiple liability

If a creditor has a claim against several debtors who are liable for the same claim, and one of the debtors has already satisfied the claim in whole or in part, the law governing the debtor's obligation towards the creditor also governs the debtor's right to claim recourse from the other debtors. The other debtors may rely on the defences they had against the creditor to the extent allowed by the law governing their obligations towards the creditor.

Article 17
Set-off

Where the right to set-off is not agreed by the parties, set-off shall be governed by the law applicable to the claim against which the right to set-off is asserted.

Article 18
Burden of proof

1. The law governing a contractual obligation under this Regulation shall apply to the extent that, in matters of contractual obligations, it contains rules which raise presumptions of law or determine the burden of proof.
2. A contract or an act intended to have legal effect may be proved by any mode of proof recognised by the law of the forum or by any of the laws referred to in Article 11 under which that contract or act is formally valid, provided that such mode of proof can be administered by the forum.

CHAPTER III
OTHER PROVISIONS

Article 19
Habitual residence

1. For the purposes of this Regulation, the habitual residence of companies and other bodies, corporate or unincorporated, shall be the place of central administration.
The habitual residence of a natural person acting in the course of his business activity shall be his principal place of business.
2. Where the contract is concluded in the course of the operations of a branch, agency or any other establishment, or if, under the contract, performance is the responsibility of such a branch, agency or establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence.
3. For the purposes of determining the habitual residence, the relevant point in time shall be the time of the conclusion of the contract.

Article 20
Exclusion of renvoi

The application of the law of any country specified by this Regulation means the application of the rules of law in force in that country other than its rules of private international law, unless provided otherwise in this Regulation.

Article 21
Public policy of the forum

The application of a provision of the law of any country specified by this Regulation may be refused only if such application is manifestly incompatible with the public policy (ordre public) of the forum.

Article 22
States with more than one legal system

1. Where a State comprises several territorial units, each of which has its own rules of law in respect of contractual obligations, each territorial unit shall be considered as a country for the purposes of identifying the law applicable under this Regulation.
2. A Member State where different territorial units have their own rules of law in respect of contractual obligations shall not be required to apply this Regulation to conflicts solely between the laws of such units.

Article 23
Relationship with other provisions of Community law

With the exception of Article 7, this Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to contractual obligations.

Article 24
Relationship with the Rome Convention

1. This Regulation shall replace the Rome Convention in the Member States, except as regards the territories of the Member States which fall within the territorial scope of that Convention and to which this Regulation does not apply pursuant to Article 299 of the Treaty.
2. In so far as this Regulation replaces the provisions of the Rome Convention, any reference to that Convention shall be understood as a reference to this Regulation.

Article 25
Relationship with existing international conventions

1. This Regulation shall not prejudice the application of international conventions to which one or more Member States are parties at the time when this Regulation is adopted and which lay down conflict-of-law rules relating to contractual obligations.
2. However, this Regulation shall, as between Member States, take precedence over conventions concluded exclusively between two or more of them in so far as such conventions concern matters governed by this Regulation.

Article 26
List of Conventions

1. By 17 June 2009, Member States shall notify the Commission of the conventions referred to in Article 25(1). After that date, Member States shall notify the Commission of all denunciations of such conventions.
2. Within six months of receipt of the notifications referred to in paragraph 1, the Commission shall publish in the Official Journal of the European Union:
   (a) a list of the conventions referred to in paragraph 1;
   (b) the denunciations referred to in paragraph 1.

Article 27
Review clause

1. By 17 June 2013, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Regulation. If appropriate, the report shall be accompanied by proposals to amend this Regulation. The report shall include:
   (a)
a study on the law applicable to insurance contracts and an
assessment of the impact of the provisions to be introduced,
if any; and
(b) an evaluation on the application of Article 6, in particular as
regards the coherence of Community law in the field of
consumer protection.

2. By 17 June 2010, the Commission shall submit to the
European Parliament, the Council and the European
Economic and Social Committee a report on the question of
the effectiveness of an assignment or subrogation of a claim
against third parties and the priority of the assigned or
subrogated claim over a right of another person. The report
shall be accompanied, if appropriate, by a proposal to amend
this Regulation and an assessment of the impact of the provisions
to be introduced.

Article 28
Application in time

This Regulation shall apply to contracts concluded after 17
December 2009.

CHAPTER IV
FINAL PROVISIONS

Article 29
Entry into force and application

This Regulation shall enter into force on the 20th day
following its publication in the Official Journal of the
European Union.

It shall apply from 17 December 2009 except for Article 26
which shall apply from 17 June 2009.

This Regulation shall be binding in its entirety and directly
applicable in the Member States in accordance with the
Treaty establishing the European Community.

Done at Strasbourg, 17 June 2008.

For the European Parliament

The President
H.-G. PÖTTERING
For the Council
The President
J. LENARCIC

Regulation (EC) No 864/2007 of the European parliament and
of the Council of 11 July 2007 on the law applicable to non-
contractual obligations (Rome II)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE
EUROPEAN UNION,

Having regard to the Treaty establishing the European
Community, and in particular Articles 61 (c) and 67 thereof,
Having regard to the proposal from the Commission,
Having regard to the opinion of the European Economic and
Social Committee (1),

Acting in accordance with the procedure laid down in Article
251 of the Treaty in the light of the joint text approved by the
Conciliation Committee on 25 June 2007 (2),

Whereas:

(1) The Community has set itself the objective of maintaining
and developing an area of freedom, security and justice. For
the progressive establishment of such an area, the
Community is to adopt measures relating to judicial
cooperation in civil matters with a cross-border impact to the
extent necessary for the proper functioning of the
internal market.
(2) According to Article 65(b) of the Treaty, these measures
are to include those promoting the compatibility of the rules
applicable in the Member States concerning the conflict of
laws and of jurisdiction.

(3) The European Council meeting in Tampere on 15 and 16
October 1999 endorsed the principle of mutual recognition
of judgments and other decisions of judicial authorities as
the cornerstone of judicial cooperation in civil matters and
invited the Council and the Commission to adopt a
programme of measures to implement the principle of
mutual recognition.

(4) On 30 November 2000, the Council adopted a joint
Commission and Council programme of measures for
implementation of the principle of mutual recognition of
decisions in civil and commercial matters (3). The
programme identifies measures relating to the
harmonisation of conflict-of-law rules as those facilitating
the mutual recognition of judgments.

(5) The Hague Programme (4), adopted by the European
Council on 5 November 2004, called for work to be pursued
actively on the rules of conflict of laws regarding non-
contractual obligations (Rome II).

(6) The proper functioning of the internal market creates a
need, in order to improve the predictability of the outcome of
litigation, certainty as to the law applicable and the free
movement of judgments, for the conflict-of-law rules in the
Member States to designate the same national law
irrespective of the country of the court in which an action is brought.

(7) The substantive scope and the provisions of this Regulation should be consistent with Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (5) (Brussels I) and the instruments dealing with the law applicable to contractual obligations.

(8) This Regulation should apply irrespective of the nature of the court or tribunal seised.

(9) Claims arising out of acts of acta iure imperii should include claims against officials who act on behalf of the State and liability for acts of public authorities, including liability of publicly appointed office-holders. Therefore, these matters should be excluded from the scope of this Regulation.

(10) Family relationships should cover parentage, marriage, affinity and collateral relatives. The reference in Article 1 (2) to relationships having comparable effects to marriage and other family relationships should be interpreted in accordance with the law of the Member State in which the court is seised.

(11) The concept of a non-contractual obligation varies from one Member State to another. Therefore for the purposes of this Regulation non-contractual obligation should be understood as an autonomous concept. The conflict-of-law rules set out in this Regulation should also cover non-contractual obligations arising out of strict liability.

(12) The law applicable should also answer the question of the capacity to incur liability in tort/delict.

(13) Uniform rules applied irrespective of the law they designate may avert the risk of distortions of competition between Community litigants.

(14) The requirement of legal certainty and the need to do justice in individual cases are essential elements of an area of justice. This Regulation provides for the connecting factors which are the most appropriate to achieve these objectives. Therefore, this Regulation provides for a general rule but also for specific rules and, in certain provisions, for an 'escape clause' which allows a departure from these rules where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with another country. This set of rules thus creates a flexible framework of conflict-of-law rules. Equally, it enables the court seised to treat individual cases in an appropriate manner.

(15) The principle of the lex loci delicti commissis is the basic solution for non-contractual obligations in virtually all the Member States, but the practical application of the principle where the component factors of the case are spread over several countries varies. This situation engenders uncertainty as to the law applicable.

(16) Uniform rules should enhance the foreseeability of court decisions and ensure a reasonable balance between the interests of the person claimed to be liable and the person who has sustained damage. A connection with the country where the direct damage occurred (lex loci damni) strikes a fair balance between the interests of the person claimed to be liable and the person sustaining the damage, and also reflects the modern approach to civil liability and the development of systems of strict liability.

(17) The law applicable should be determined on the basis of where the damage occurs, regardless of the country or countries in which the indirect consequences could occur. Accordingly, in cases of personal injury or damage to property, the country in which the damage occurs should be the country where the injury was sustained or the property was damaged respectively.

(18) The general rule in this Regulation should be the lex loci damni provided for in Article 4(1). Article 4(2) should be seen as an exception to this general principle, creating a special connection where the parties have their habitual residence in the same country. Article 4(3) should be understood as an 'escape clause' from Article 4(1) and (2), where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with another country.

(19) Specific rules should be laid down for special torts/delicts where the general rule does not allow a reasonable balance to be struck between the interests at stake.

(20) The conflict-of-law rule in matters of product liability should meet the objectives of fairly spreading the risks inherent in a modern high-technology society, protecting consumers' health, stimulating innovation, securing undistorted competition and facilitating trade. Creation of a cascade system of connecting factors, together with a foreseeability clause, is a balanced solution in regard to these objectives. The first element to be taken into account is the law of the country in which the person sustaining the damage had his or her habitual residence when the damage occurred, if the product was marketed in that country. The other elements of the cascade are triggered if the product was not marketed in that country, without prejudice to Article 4(2) and to the possibility of a manifestly closer connection to another country.

(21) The special rule in Article 6 is not an exception to the general rule in Article 4(1) but rather a clarification of it. In matters of unfair competition, the conflict-of-law rule should protect competitors, consumers and the general public and ensure that the market economy functions properly. The connection to the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected, generally satisfies these objectives.

(22) The non-contractual obligations arising out of restrictions of competition in Article 6(3) should cover infringements of both national and Community competition law. The law applicable to such non-contractual obligations should be the law of the country where the market is, or is likely to be, affected. In cases where the market is, or is likely to be, affected in more than one country, the claimant should be able in certain circumstances to choose to base his or her claim on the law of the court seised.

(23) For the purposes of this Regulation, the concept of restriction of competition should cover prohibitions on agreements between undertakings, decisions by associations of undertakings and concerted practices which have as their object or effect the prevention, restriction or distortion of competition within a Member State or within the internal market, as well as prohibitions on the abuse of a dominant position within a Member State or within the internal market, where such agreements, decisions, concerted practices or abuses are prohibited by Articles 81 and 82 of the Treaty or by the law of a Member State.

(24) Environmental damage should be understood as meaning adverse change in a natural resource, such as water, land or air, impairment of a function performed by that resource for the benefit of another natural resource or the public, or impairment of the variability among living organisms.

(25) Regarding environmental damage, Article 174 of the Treaty, which provides that there should be a high level of protection based on the precautionary principle and the principle that preventive action should be taken, the principle of priority for corrective action at source and the principle that the polluter pays, fully justifies the use of the principle of discriminating in favour of the person sustaining the damage. The question of whether the person seeking compensation can make the choice of the law applicable should be determined in accordance with the law of the Member State in which the court is seised.

(26) Regarding infringements of intellectual property rights, the universally acknowledged principle of the lex loci protectionis should be preserved. For the purposes of this Regulation, the term 'intellectual property rights' should be interpreted as meaning, for instance, copyright, related rights, the sui generis right for the protection of databases and industrial property rights.
(27) The exact concept of industrial action, such as strike action or lock-out, varies from one Member State to another and is governed by each Member State’s internal rules. Therefore, this Regulation assumes as a general principle that the law of the country where the industrial action was taken should apply, with the aim of protecting the rights and obligations of workers and employers.

(28) The special rule on industrial action in Article 9 is without prejudice to the conditions relating to the exercise of such action in accordance with national law and without prejudice to the legal status of trade unions or of the representative organisations of workers as provided for in the law of the Member States.

(29) Provision should be made for special rules where damage is caused by an act other than a tort/delict, such as unjust enrichment, negotorium gestio and culpa in contrahendo.

(30) Culpa in contrahendo for the purposes of this Regulation is an autonomous concept and should not necessarily be interpreted within the meaning of national law. It should include the violation of the duty of disclosure and the breakdown of contractual negotiations. Article 12 covers only non-contractual obligations presenting a direct link with the dealings prior to the conclusion of a contract. This means that if, while a contract is being negotiated, a person suffers personal injury, Article 4 or other relevant provisions of this Regulation should apply.

(31) To respect the principle of party autonomy and to enhance legal certainty, the parties should be allowed to make a choice as to the law applicable to a non-contractual obligation. This choice should be expressed or demonstrated with reasonable certainty by the circumstances of the case. Where establishing the existence of the agreement, the court has to respect the intentions of the parties. Protection should be given to weaker parties by imposing certain conditions on the choice.

(32) Considerations of public interest justify giving the courts of the Member States the possibility, in exceptional circumstances, of applying exceptions based on public policy and overriding mandatory provisions. In particular, the application of a provision of the law designated by this Regulation which would have the effect of causing non-compensatory exemplary or punitive damages of an excessive nature to be awarded may, depending on the circumstances of the case and the legal order of the Member State of the court seised, be regarded as being contrary to the public policy (ordre public) of the forum.

(33) According to the current national rules on compensation awarded to victims of road traffic accidents, when quantifying damages for personal injury in cases in which the accident takes place in a State other than that of the habitual residence of the victim, the court seised should take into account all the relevant actual circumstances of the specific victim, including in particular the actual losses and costs of after-care and medical attention.

(34) In order to strike a reasonable balance between the parties, account must be taken, in so far as appropriate, of the rules of safety and conduct in operation in the country in which the harmful act was committed, even where the non-contractual obligation is governed by the law of another country. The term ‘rules of safety and conduct’ should be interpreted as referring to all regulations having any relation to safety and conduct, including, for example, road safety rules in the case of an accident.

(35) A situation where conflict-of-law rules are dispersed among several instruments and where there are differences between those rules should be avoided. This Regulation, however, does not exclude the possibility of inclusion of conflict-of-law rules relating to non-contractual obligations in provisions of Community law with regard to particular matters. This Regulation should not prejudice the application of other instruments laying down provisions designed to contribute to the proper functioning of the internal market in so far as they cannot be applied in conjunction with the law designated by the rules of this Regulation. The application of provisions of the applicable law designated by the rules of this Regulation should not restrict the free movement of goods and services as regulated by Community instruments, such as Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (6).

(36) Respect for international commitments entered into by the Member States means that this Regulation should not affect international conventions to which one or more Member States are parties at the time this Regulation is adopted. To make the rules more accessible, the Commission should publish the list of the relevant conventions in the Official Journal of the European Union on the basis of information supplied by the Member States.

(37) The Commission will make a proposal to the European Parliament and the Council concerning the procedures and conditions according to which Member States would be entitled to negotiate and conclude on their own behalf agreements with third countries in individual and exceptional cases, concerning sectoral matters, containing provisions on the law applicable to non-contractual obligations. Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can, therefore, by reason of the scale and effects of this Regulation, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity set out in Article 5 of the Treaty. In accordance with the principle of proportionality set out in that Article, this Regulation does not go beyond what is necessary to attain that objective.

(39) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, the United Kingdom and Ireland are taking part in the adoption and application of this Regulation.

(40) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark does not take part in the adoption of this Regulation, and is not bound by it or subject to its application.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SCOPE

Article 1

Scope

1. This Regulation shall apply, in situations involving a conflict of laws, to non-contractual obligations in civil and commercial matters. It shall not apply, in particular, to revenue, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (acta iure imperii).

2. The following shall be excluded from the scope of this Regulation:
(a) non-contractual obligations arising out of family relationships and relationships deemed by the law applicable to such relationships to have comparable effects including maintenance obligations;
(b) non-experimental obligations arising out of matrimonial property regimes, property regimes of relationships deemed by the law applicable to such relationships to have comparable effects to marriage, and wills and succession;
(c) non-contractual obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations...
under such other negotiable instruments arise out of their negotiable character;
(d) non-contractual obligations arising out of the law of companies and other bodies corporate or unincorporated regarding matters such as the creation, by registration or otherwise, legal capacity, internal organisation or winding up of companies and other bodies corporate or unincorporated, the personal liability of officers and members as such for the obligations of the company or body and the personal liability of auditors to a company or to its members in the statutory audits of accounting documents;
(e) non-contractual obligations arising out of the relations between the settlors, trustees and beneficiaries of a trust created voluntarily;
(f) non-contractual obligations arising out of nuclear damage;
(g) non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.
3. This Regulation shall not apply to evidence and procedure, without prejudice to Articles 21 and 22.
4. For the purposes of this Regulation, 'Member State' shall mean any Member State other than Denmark.

Article 2
Non-contractual obligations
1. For the purposes of this Regulation, damage shall cover any consequence arising out of tort/delict, unjust enrichment, negotiorum gestio or culpa in contrahendo.
2. This Regulation shall apply also to non-contractual obligations that are likely to arise.
3. Any reference in this Regulation to:
   (a) an event giving rise to damage shall include events giving rise to damage that are likely to occur; and
   (b) damage shall include damage that is likely to occur.

Article 3
Universal application
Any law specified by this Regulation shall be applied whether or not it is the law of a Member State.

CHAPTER II
TORTS/DELICTS

Article 4
General rule
1. Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.
2. However, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply.
3. Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.

Article 5
Product liability
1. Without prejudice to Article 4(2), the law applicable to a non-contractual obligation arising out of damage caused by a product shall be:
   (a) the law of the country in which the person sustaining the damage had his or her habitual residence when the damage occurred, if the product was marketed in that country; or, failing that,
   (b) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that,
   (c) the law of the country in which the damage occurred, if the product was marketed in that country.
   However, the law applicable shall be the law of the country in which the person claimed to be liable is habitually resident if he or she could not reasonably foresee the marketing of the product, or a product of the same type, in the country the law of which is applicable under (a), (b) or (c).
2. Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraph 1, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.

Article 6
Unfair competition and acts restricting free competition
1. The law applicable to a non-contractual obligation arising out of an act of unfair competition shall be the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected.
2. Where an act of unfair competition affects exclusively the interests of a specific competitor, Article 4 shall apply.
3. (a) The law applicable to a non-contractual obligation arising out of a restriction of competition shall be the law of the country where the market is, or is likely to be, affected.
   (b) When the market is, or is likely to be, affected in more than one country, the person seeking compensation for damage who sues in the court of the domicile of the defendant, may instead choose to base his or her claim on the law of the court seised, provided that the market in that Member State is amongst those directly and substantially affected by the restriction of competition out of which the non-contractual obligation on which the claim is based arises; where the claimant sues, in accordance with the applicable rules on jurisdiction, more than one defendant in that court, he or she can only choose to base his or her claim on the law of that court if the restriction of competition on which the claim against each of these defendants relies directly and substantially affects also the market in the Member State of that court.
4. The law applicable under this Article may not be derogated from by an agreement pursuant to Article 14.

Article 7
Environmental damage
The law applicable to a non-contractual obligation arising out of environmental damage or damage sustained by persons or property as a result of such damage shall be the law determined pursuant to Article 4(1), unless the person seeking compensation for damage chooses to base his or her claim on the law of the country in which the event giving rise to the damage occurred.

Article 8
Infringement of intellectual property rights
1. The law applicable to a non-contractual obligation arising from an infringement of an intellectual property right shall be the law of the country for which protection is claimed.
2. In the case of a non-contractual obligation arising from an infringement of a unitary Community intellectual property right, the law applicable shall, for any question that is not
governed by the relevant Community instrument, be the law of the country in which the act of infringement was committed.

3. The law applicable under this Article may not be derogated from by an agreement pursuant to Article 14.

Article 9

Industrial action

Without prejudice to Article 4(2), the law applicable to a non-contractual obligation in respect of the liability of a person in the capacity of a worker or an employer or the organisations representing their professional interests for damages caused by an industrial action, pending or carried out, shall be the law of the country where the action is to be, or has been taken.

CHAPTER III
UNJUST ENRICHMENT, NEGOTIORUM GESTIO AND CULPA IN CONTRAHENDO

Article 10
Unjust enrichment

1. If a non-contractual obligation arising out of unjust enrichment, including payment of amounts wrongly received, concerns a relationship existing between the parties, such as one arising out of a contract or a tort/delict, that is closely connected with that unjust enrichment, it shall be governed by the law that governs that relationship.

2. Where the law applicable cannot be determined on the basis of paragraph 1 and the parties have their habitual residence in the same country when the event giving rise to unjust enrichment occurs, the law of that country shall apply.

3. Where the law applicable cannot be determined on the basis of paragraphs 1 or 2, it shall be the law of the country in which the unjust enrichment took place.

4. Where it is clear from all the circumstances of the case that the non-contractual obligation arising out of unjust enrichment is manifestly more closely connected with a country other than that indicated in paragraphs 1, 2 and 3, the law of that other country shall apply.

Article 11
Negotiorum gestio

1. If a non-contractual obligation arising out of an act performed without due authority in connection with the affairs of another person concerns a relationship existing between the parties, such as one arising out of a contract or a tort/delict, that is closely connected with that non-contractual obligation, it shall be governed by the law that governs that relationship.

2. Where the law applicable cannot be determined on the basis of paragraph 1, and the parties have their habitual residence in the same country when the event giving rise to the damage occurs, the law of that country shall apply.

3. Where the law applicable cannot be determined on the basis of paragraphs 1 or 2, it shall be the law of the country in which the act was performed.

4. Where it is clear from all the circumstances of the case that the non-contractual obligation arising out of an act performed without due authority in connection with the affairs of another person is manifestly more closely connected with a country other than that indicated in paragraphs 1, 2 and 3, the law of that other country shall apply.

Article 12
Culpa in contrahendo

1. The law applicable to a non-contractual obligation arising out of dealings prior to the conclusion of a contract, regardless of whether the contract was actually concluded or not, shall be the law that applies to the contract or that would have been applicable to it had it been entered into.

2. Where the law applicable cannot be determined on the basis of paragraph 1, it shall be:

(a) the law of the country in which the damage occurs, irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occurred; or

(b) where the parties have their habitual residence in the same country at the time when the event giving rise to the damage occurs, the law of that country; or

(c) where it is clear from all the circumstances of the case that the non-contractual obligation arising out of dealings prior to the conclusion of a contract is manifestly more closely connected with a country other than that indicated in points (a) and (b), the law of that other country.
1. The question whether a right to claim damages or a remedy may be transferred, including by inheritance;
2. (f) persons entitled to compensation for damage sustained personally;
3. (g) liability for the acts of another person;
4. (h) the manner in which an obligation may be extinguished and rules of prescription and limitation, including rules relating to the commencement, interruption and suspension of a period of prescription or limitation.

Article 16

Overriding mandatory provisions

Nothing in this Regulation shall restrict the application of the provisions of the law of the forum in a situation where they are mandatory irrespective of the law otherwise applicable to the non-contractual obligation.

Article 17

Rules of safety and conduct

In assessing the conduct of the person claimed to be liable, account shall be taken, as a matter of fact and in so far as is appropriate, of the rules of safety and conduct which were in force at the place and time of the event giving rise to the liability.

Article 18

Direct action against the insurer of the person liable

The person having suffered damage may bring his or her claim directly against the insurer of the person liable to provide compensation if the law applicable to the non-contractual obligation or the law applicable to the insurance contract so provides.

Article 19

Subrogation

Where a person (the creditor) has a non-contractual claim upon another (the debtor), and a third person has a duty to satisfy the creditor, or has in fact satisfied the creditor in discharge of that duty, the law which governs the third person’s duty to satisfy the creditor shall determine whether, and the extent to which, the third person is entitled to exercise against the debtor the rights which the creditor had against the debtor under the law governing their relationship.

Article 20

Multiple liability

If a creditor has a claim against several debtors who are liable for the same claim, and one of the debtors has already satisfied the claim in whole or in part, the question of that debtor’s right to demand compensation from the other debtors shall be governed by the law applicable to that debtor’s non-contractual obligation towards the creditor.

Article 21

Formal validity

A unilateral act intended to have legal effect and relating to a non-contractual obligation shall be formally valid if it satisfies the formal requirements of the law governing the non-contractual obligation in question or the law of the country in which the act is performed.

Article 22

Burden of proof

1. The law governing a non-contractual obligation under this Regulation shall apply to the extent that, in matters of non-contractual obligations, it contains rules which raise presumptions of law or determine the burden of proof.
2. Acts intended to have legal effect may be proved by any mode of proof recognised by the law of the forum or by any of the laws referred to in Article 21 under which that act is formally valid, provided that such mode of proof can be administered by the forum.

CHAPTER VI

OTHER PROVISIONS

Article 23

Habitual residence
1. For the purposes of this Regulation, the habitual residence of companies and other bodies, corporate or unincorporated, shall be the place of central administration.
2. Where the event giving rise to the damage occurs, or the damage arises, in the course of operation of a branch, agency or any other establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence.

Article 24

Exclusion of renvoi

The application of the law of any country specified by this Regulation means the application of the rules of law in force in that country other than its rules of private international law.

Article 25

States with more than one legal system
1. Where a State comprises several territorial units, each of which has its own rules of law in respect of non-contractual obligations, each territorial unit shall be considered as a country for the purposes of identifying the law applicable under this Regulation.
2. A Member State within which different territorial units have their own rules of law in respect of non-contractual obligations shall not be required to apply this Regulation to conflicts solely between the laws of such units.

Article 26

Public policy of the forum

The application of a provision of the law of any country specified by this Regulation may be refused only if such application is manifestly incompatible with the public policy (ordre public) of the forum.

Article 27

Relationship with other provisions of Community law

This Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to non-contractual obligations.

Article 28

Relationship with existing international conventions
1. This Regulation shall not prejudice the application of international conventions to which one or more Member States are parties at the time when this Regulation is adopted and which lay down conflict-of-law rules relating to non-contractual obligations.
2. However, this Regulation shall, as between Member States, take precedence over conventions concluded exclusively between two or more of them in so far as such conventions concern matters governed by this Regulation.
CHAPTER VII
FINAL PROVISIONS

Article 29
List of conventions
1. By 11 July 2008, Member States shall notify the Commission of the conventions referred to in Article 28(1). After that date, Member States shall notify the Commission of all denunciations of such conventions.
2. The Commission shall publish in the Official Journal of the European Union within six months of receipt:
   (i) a list of the conventions referred to in paragraph 1;
   (ii) the denunciations referred to in paragraph 1.

Article 30
Review clause
1. Not later than 20 August 2011, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Regulation. If necessary, the report shall be accompanied by proposals to adapt this Regulation. The report shall include:
   (i) a study on the effects of the way in which foreign law is treated in the different jurisdictions and on the extent to which courts in the Member States apply foreign law in practice pursuant to this Regulation;
   (ii) a study on the effects of Article 28 of this Regulation with respect to the Hague Convention of 4 May 1971 on the law applicable to traffic accidents.
2. Not later than 31 December 2008, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a study on the situation in the field of the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, taking into account rules relating to freedom of the press and freedom of expression in the media, and conflict-of-law issues related to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (7).

Article 31
Application in time
This Regulation shall apply to events giving rise to damage which occur after its entry into force.

Article 32
Date of application
This Regulation shall apply from 11 January 2009, except for Article 29, which shall apply from 11 July 2008.

For the European Parliament
The President
H.-G. PÖTTERING

For the Council
The President
M. LOBO ANTUNES


Commission Statement on the review clause (Article 30)
The Commission, following the invitation by the European Parliament and the Council in the frame of Article 30 of the ‘Rome II’ Regulation, will submit, not later than December 2008, a study on the situation in the field of the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality. The Commission will take into consideration all aspects of the situation and take appropriate measures if necessary.
EUROPEAN ICT LAW 2015
Casebook
Michal Koščík, Radim Polčák, Jakub Harašta, Václav Stupka, Matěj Myška, Libor Kyncl

Published and printed by Tribun EU, s. r. o. 
Čejl 892/32, 602 00 Brno

First edition in Tribun EU

Brno 2015
