Legislation selection IT&Law *IT & Law 2019-2020*

Part I: Computer Systems (CS) + Finance for engineers/BIT

1. DIRECTIVE 2009/24/EC on the legal protection of computer programs
2. DIRECTIVE 96/9/EC on the legal protection of databases
3. REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
4. DIRECTIVE 2013/40/EU on attacks against information systems
5. DUTCH CRIMINAL CODE (computer crime selection)

Part II: Finance for engineers/BIT ONLY

6. DIRECTIVE 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
7. DIRECTIVE 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
8. DIRECTIVE 2006/123/EC on services in the internal market
9. DIRECTIVE 2011/83/EU on consumer rights

DIRECTIVES

DIRECTIVE 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 April 2009

on the legal protection of computer programs

(Codified version)

(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) The content of Council Directive 91/250/EEC of 14 May 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 design 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.

[1] OJ C 204, 9.8.2008, p. 24.
[2] Opinion of the European Parliament of 17 June 2008 (not yet published in the Official Journal) and Council Decision of 23 March 2009.
[3] OJ L 122, 17.5.1991, p. 42.
[4] See Annex I, Part A.

(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, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as 'interfaces'. This functional interconnection and interaction is generally known as 'interoperability'; such interoperability can 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 loading 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 deemed 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 observation, 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

Decompilation

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 rights, trade-marks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract.

Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5(2) and (3) shall be null and void.

Article 9

Communication

Member States shall communicate to the Commission the provisions of national law adopted in the field governed by this Directive.

Article 10

Repeal

Directive 91/250/EEC, as amended by the Directive indicated in Annex I, Part A, is repealed, 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.

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 11

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 12

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 23 April 2009.

For the European Parliament	*For the Council*
The President	*The President*
H.-G. PÖTTERING	P. NEČAS

ANNEX I

PART A

Repealed Directive with its amendment

(referred to in Article 10)

Council Directive 91/250/EEC
(OJ L 122, 17.5.1991, p. 42)

Council Directive 93/98/EEC (OJ L 290, 24.11.1993, p. 9) — Article 11(1) only

PART B

List of time-limits for transposition into national law

(referred to in Article 10)

Directive	Time-limit for transposition
91/250/EEC	31 December 1992
93/98/EEC	30 June 1995

ANNEX II

Correlation table

Directive 91/250/EEC	This Directive
Article 1(1), (2) and (3)	Article 1(1), (2) and (3)
Article 2(1), first sentence	Article 2(1), first subparagraph
Article 2(1), second sentence	Article 2(1), second subparagraph
Article 2(2) and (3)	Article 2(2) and (3)
Article 3	Article 3
Article 4, introductory words	Article 4(1), introductory words
Article 4(a)	Article 4(1), point (a)
Article 4(b)	Article 4(1), point (b)
Article 4(c), first sentence	Article 4(1), point (c)
Article 4(c), second sentence	Article 4(2)
Articles 5, 6 and 7	Articles 5, 6 and 7
Article 9(1), first sentence	Article 8, first paragraph
Article 9(1), second sentence	Article 8, second paragraph
Article 9(2)	Article 1(4)
Article 10(1)	—
Article 10(2)	Article 9
—	Article 10
—	Article 11
Article 11	Article 12
—	Annex I
—	Annex II

DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 11 March 1996

on the legal protection of databases

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 will also be of use 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;

(1) OJ No C 156, 23. 6. 1992, p. 4 and OJ No C 308, 15. 11. 1993, p. 1.
(2) OJ No C 19, 25. 1. 1993, p. 3.
(3) Opinion of the European Parliament of 23 June 1993 (OJ No C 194, 19. 7. 1993, p. 144), Common Position of the Council of 10 July 1995 (OJ No C 288, 30. 10. 1995, p. 14), Decision of the European Parliament of 14 December 1995 (OJ No C 17, 22 1. 1996) and Council Decision of 26 February 1996.

(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, cinematographic, 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 subject to the required consent of the author or of the holder of the related right without the *sui generis* right of 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 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 not be taken to extend 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 [1];

(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 intellectual property [2];

(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 [3];

(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

[1] OJ No L 122, 17. 5. 1991, p. 42. Directive as last amended by Directive 93/98/EEC (OJ No L 290, 24. 11. 1993, p. 9.)
[2] OJ No L 346, 27. 11. 1992, p. 61.
[3] OJ No L 290, 24. 11. 1993, p. 9.

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;

(28) 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;

(29) 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;

(30) Whereas the author's exclusive rights should include the right to determine the way in which his work is exploited and by whom, and in particular to control the distribution of his work to unauthorized persons;

(31) Whereas the copyright protection of databases includes making databases available by means other than the distribution of copies;

(32) 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;

(33) 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;

(34) 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;

(35) 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;

(36) Whereas the term 'scientific research' within the meaning of this Directive covers both the natural sciences and the human sciences;

(37) Whereas Article 10 (1) of the Berne Convention is not affected by this Directive;

(38) 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;

(39) 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;

(40) 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;

(41) 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;

(42) 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;

(43) 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;

(44) 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;

(45) Whereas the right to prevent unauthorized extraction and/or re-utilization does not in any way constitute an extension of copyright protection to mere facts or data;

(46) 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;

(47) 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 ditribution 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;

(48) 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 [1], 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;

(49) 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 institution;

[1] OJ No L 281, 23. 11. 1995, p. 31.

(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,

HAVE 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 rightholder 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 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 curtailing 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 refered 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.

Article 17

This Directive is addressed to the Member States.

Done at Strasbourg, 11 March 1996.

For the European Parliament	*For the Council*
The President	*The President*
K. HÄNSCH	L. DINI

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(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 16 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]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council ([4]) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

([1]) OJ C 229, 31.7.2012, p. 90.
([2]) OJ C 391, 18.12.2012, p. 127.
([3]) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
([4]) 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 (OJ L 281, 23.11.1995, p. 31).

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate 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.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC ([1]).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

([1]) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

([2]) 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 L 8, 12.1.2001, p. 1).

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council ([1]). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council ([2]), in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

([1]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

([2]) 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') (OJ L 178, 17.7.2000, p. 1).

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council ([1]) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be

([1]) 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 (OJ L 88, 4.4.2011, p. 45).

the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or

Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([1]) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law 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 authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data

([1]) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. 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 personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their

further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, 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, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes

by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council ([1]), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

([1]) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given

his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because 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 on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the

nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data

protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out

and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of

protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council ([1]) as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the

([1]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require 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. In the latter case, such a transfer should not involve the entirety of the personal 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, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the

processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the

possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance

with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first

seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council [1] should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate

[1] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council ([1]) leaves intact and in no way affects the level of protection of natural persons with regard to the

([1]) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access 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 provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council ([1]) should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council ([2]) provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement

([1]) Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

([2]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. 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.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or 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 (TEU). 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.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 ([1]).

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à-vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ([2]), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

([1]) OJ C 192, 30.6.2012, p. 7.

([2]) 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) (OJ L 201, 31.7.2002, p. 37).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) '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;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1];

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(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;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific

processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council [1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(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 another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law 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 a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([1]).

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

([1]) 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 (OJ L 145, 31.5.2001, p. 43).

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

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 delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication 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 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three 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 three months at the initiative of the European Parliament or of the Council.

Article 93

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.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to 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 shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

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. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 August 2013

on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

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 83(1) 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) The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

(2) Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(3) Attacks against information systems, and, in particular, attacks linked to organised crime, are a growing menace in the Union and globally, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and of the Union. This constitutes a threat to the achievement of a safer information society and of an area of freedom, security, and justice, and therefore requires a response at Union level and improved cooperation and coordination at international level.

(4) There are a number of critical infrastructures in the Union, the disruption or destruction of which would have a significant cross-border impact. It has become apparent from the need to increase the critical infrastructure protection capability in the Union that the measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks. Critical infrastructure could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(5) There is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which can often be critical to Member States or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage alone could pose a serious risk to public interests. This Directive aims, inter alia, to introduce criminal penalties for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information.

(6) Large-scale cyber attacks can cause substantial economic damage both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their vulnerability to such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

([1]) OJ C 218, 23.7.2011, p. 130.

([2]) Position of the European Parliament of 4 July 2013 (not yet published in the Official Journal) and decision of the Council of 22 July 2013.

(7) Common definitions in this area are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(8) There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

(9) Interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

(10) Member States should provide for penalties in respect of attacks against information systems. Those penalties should be effective, proportionate and dissuasive and should include imprisonment and/or fines.

(11) This Directive provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

(12) The identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps.

(13) It is appropriate to provide for more severe penalties where an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime ([1]), where a cyber attack is conducted on a large scale, thus affecting a significant number of information systems, including where it is intended to create a botnet, or where a cyber attack causes serious damage, including where it is carried out through a botnet. It is also appropriate to provide for more severe penalties where an attack is conducted against a critical infrastructure of the Member States or of the Union.

(14) Setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime. Any need for Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.

(15) The Council Conclusions of 27 to 28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention. Completing the process of ratification of that Convention by all Member States as soon as possible should be considered to be a priority.

(16) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive refers to tools that can be used in order to commit the offences laid down in this Directive. Such tools could include malicious software, including those able to create botnets, used to commit cyber attacks. Even where such a tool is suitable or particularly suitable for carrying out one of the offences laid down in this Directive, it is possible that it was produced for a legitimate purpose Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as to test the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be used to commit one or more of the offences laid down in this Directive must be also fulfilled.

(17) This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. This Directive is without prejudice to the right of access to information as laid down in national and Union law, while at the same time it may not serve as a justification for unlawful or arbitrary access to information.

([1]) OJ L 300, 11.11.2008, p. 42.

(18) Cyber attacks could be facilitated by various circumstances, such as where the offender has access to security systems inherent in the affected information systems within the scope of his or her employment. In the context of national law, such circumstances should be taken into account in the course of criminal proceedings as appropriate.

(19) Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders. It remains within the discretion of the judge to assess those circumstances together with the other facts of the particular case.

(20) This Directive does not govern conditions for exercising jurisdiction over any of the offences referred to herein, such as a report by the victim in the place where the offence was committed, a denunciation from the State of the place where the offence was committed, or the non-prosecution of the offender in the place where the offence was committed.

(21) In the context of this Directive, States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations.

(22) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a 24 hour, seven-day-a-week basis. Those points of contact should be able to deliver effective assistance thus, for example, facilitating the exchange of relevant information available and the provision of technical advice or legal information for the purpose of investigations or proceedings concerning criminal offences relating to information systems and associated data involving the requesting Member State. In order to ensure the smooth operation of the networks, each contact point should have the capacity to communicate with the point of contact of another Member State on an expedited basis with the support, inter alia, of trained and equipped personnel. Given the speed with which large-scale cyber attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. In such cases, it may be expedient that the request for information be accompanied by telephone contact in order to ensure that the request is processed swiftly by the requested Member State and that feedback is provided within eight hours.

(23) Cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive.

(24) There is a need to collect comparable data on the offences laid down in this Directive. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby to contribute to formulating a more effective response. Member States should submit information on the modus operandi of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) [1]. Providing information can facilitate a better understanding of present and future threats and thus contribute to more appropriate and targeted decision-making on combating and preventing attacks against information systems.

(25) The Commission should submit a report on the application of this Directive and make necessary legislative proposals which could lead to broadening its scope, taking into account developments in the field of cybercrime. Such developments could include technological developments, for example those enabling more effective enforcement in the area of attacks against information systems or facilitating prevention or minimising the impact of such attacks. For that purpose, the Commission should take into account the available analyses and reports produced by relevant actors and, in particular, Europol and ENISA.

(26) In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks. Member States should take the necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection

[1] OJ L 121, 15.5.2009, p. 37.

and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(27) Significant gaps and differences in Member States' laws and criminal procedures in the area of attacks against information systems may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area. In addition, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adequate implementation and application of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings ([1]). Member States, in cooperation with the Union, should also seek to improve international cooperation relating to the security of information systems, computer networks and computer data. Proper consideration of the security of data transfer and storage should be given in any international agreement involving data exchange.

(28) Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective fight against cybercrime. In this context, stepping up the efforts to provide adequate training to the relevant authorities in order to raise the understanding of cybercrime and its impact, and to foster cooperation and the exchange of best practices, for example via the competent specialised Union agencies and bodies, should be encouraged. Such training should, inter alia, aim at raising awareness about the different national legal systems, the possible legal and technical challenges of criminal investigations, and the distribution of competences between the relevant national authorities.

(29) This Directive respects human rights and fundamental freedoms and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, including the protection of personal data, the right to privacy, freedom of expression and information, the right to a fair trial, the presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for those rights and principles and must be implemented accordingly.

(30) The protection of personal data is a fundamental right in accordance with Article 16(1) TFEU and Article 8 of the Charter on Fundamental Rights of the European Union. Therefore, any processing of personal data in the context of the implementation of this Directive should fully comply with the relevant Union law on data protection.

(31) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, those Member States have notified their wish to take part in the adoption and application of this Directive.

(32) 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 on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(33) Since the objectives of this Directive, namely to subject attacks against information systems in all Member States to effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between judicial and other competent authorities, cannot be sufficiently achieved by the Member States, and can therefore, by reason of their scale or effects, 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.

(34) This Directive aims to amend and expand the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems ([2]). Since the amendments to be made are of substantial number and nature, Framework Decision 2005/222/JHA should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive,

([1]) OJ L 328, 15.12.2009, p. 42.

([2]) OJ L 69, 16.3.2005, p. 67.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) 'information system' means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

(b) 'computer data' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function;

(c) 'legal person' means an entity having the status of legal person under the applicable law, but does not include States or public bodies acting in the exercise of State authority, or public international organisations;

(d) 'without right' means conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

Article 3

Illegal access to information systems

Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 5

Illegal data interference

Member States shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 7

Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8

Incitement, aiding and abetting and attempt

1. Member States shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence.

Article 9

Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant

number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:

(a) they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;

(b) they cause serious damage; or

(c) they are committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

Article 10

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following:

(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. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. The liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 11

Sanctions against legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, 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;

(d) judicial winding-up;

(e) temporary or permanent closure of establishments which have been used for committing the offence.

2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(2) is punishable by effective, proportionate and dissuasive sanctions or other measures.

Article 12

Jurisdiction

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

(a) in whole or in part within their territory; or

(b) by one of their nationals, at least in cases where the act is an offence where it was committed.

2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction 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 shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where:

(a) the offender has his or her habitual residence in its territory; or

(b) the offence is committed for the benefit of a legal person established in its territory.

Article 13

Exchange of information

1. For the purpose of exchanging information relating to the offences referred to in Articles 3 to 8, Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer.

2. Member States shall inform the Commission of their appointed point of contact referred to in paragraph 1. The Commission shall forward that information to the other Member States and competent specialised Union agencies and bodies.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Article 3 to 6 to the competent national authorities without undue delay.

Article 14

Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 7.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover existing data on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 7.

3. Member States shall transmit the data collected pursuant to this Article to the Commission. The Commission shall ensure that a consolidated review of the statistical reports is published and submitted to the competent specialised Union agencies and bodies.

Article 15

Replacement of Framework Decision 2005/222/JHA

Framework Decision 2005/222/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive, without prejudice to the obligations of the Member States relating to the time limit for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Article 16

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 4 September 2015.

2. Member States shall transmit to the Commission the text of the measures transposing into their national law the obligations imposed on them under this Directive.

3. When Member States adopt those 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 a reference shall be laid down by the Member States.

Article 17

Reporting

The Commission shall, by 4 September 2017, submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. The Commission shall also take into account the technical and legal developments in the field of cybercrime, particularly with regard to the scope of this Directive.

Article 18

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 19

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels, 12 August 2013.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	L. LINKEVIČIUS

Dutch Criminal Code

Warning: this is not an official translation. Under all circumstances the original text in Dutch language of the Criminal Code (Wetboek van Strafrecht) prevails. The State accepts no liability for damage of any kind resulting from the use of this translation.

Criminal Code

(Text valid on: 01-10-2012)

Act of 3 March 1881

We WILLEM III, by the grace of God, King of the Netherlands, Prince of Orange-Nassau, Grand Duke of Luxemburg etc. etc. etc.

Greetings to all who shall see or hear these presents! Be it known:
Whereas We have considered that it is necessary to enact a new Criminal Code;

We therefore, having heard the Council of State, and in consultation with the States General, have approved and decreed as We hereby approve and decree, to establish the following provisions which shall constitute the Criminal Code:

Book One. General Provisions
(…)

Book Two. Serious Offences
(…)

Part V. Serious Offences against Public Order

(…)

Section 138ab

1. Any person who intentionally and unlawfully gains entry to a computerised device or system or a part thereof shall be guilty of computer trespass and shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category. Unlawful entry shall be deemed to have been committed if access to the computerised device or system is gained:

a. by breaching a security measure,
b. by a technical intervention,
c. by means of false signals or a false key, or
d. by assuming a false identity.

2. Computer trespass shall be punishable by a term of imprisonment not exceeding four years or a

fine of the fourth category, if the offender subsequently copies the data stored, processed or transferred by means of the computerised device or system, which he has unlawfully accessed, and copies, intercepts or records such data for his own use or that of another.

3. Computer trespass committed via a public telecommunication network shall be punishable by a term of imprisonment not exceeding four years or a fine of the fourth category, if the offender subsequently

a. with the intention of benefitting himself or another unlawfully, uses processing capacity of a computerised device or system;
b. accesses the computerised device or system of a third party via the computerised device or system to which he has unlawfully gained entry.

Section 138b

Any person who intentionally and unlawfully hinders the access to or use of a computerised device or system by offering or sending data to it shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category.

Section 139

1. Any person who unlawfully enters a room or premises designated for public service, or who, unlawfully remaining there, does not leave immediately after having been directed to do so by the competent official, shall be liable to a term of imprisonment not exceeding three months or a fine of the second category.

2. Any person who has gained access by means of forcible entry or climbing in, or by false keys, a false order or a false uniform, or who, having entered without the prior knowledge of the competent official and not by mistake, is found there at night-time, shall be deemed to have unlawfully entered.

3. If he utters threats or employs means that could cause fear, he shall be liable to a term of imprisonment not exceeding one year or a fine of the third category.

4. The terms of imprisonment prescribed in subsections (1) and (3) may be increased by one third if two or more persons commit the serious offence in concert.

Section 139a

1. Any person who, by means of a technical device, intentionally:

1°. eavesdrops on a conversation taking place in a dwelling or enclosed room or premises without having been instructed to do so by a participant in that conversation;
2°. records that conversation without being a participant in it and without having been instructed to do so by such a participant;

shall be liable to a term of imprisonment not exceeding six months or a fine of the fourth category.

2. Subsection (1) shall not apply to the recording:

1°. of data that is processed or transferred by means of telecommunication or by means of a computerised device or system;
2°. by means of a technical device that is in place and is not concealed, on the authority of the person who uses the dwelling or enclosed room or premises, except in cases of obvious misuse;
3°. for the purpose of implementation of the Intelligence and Security Services Act 2002 [*Wet op*

de Inlichtingen- en Veiligheidsdiensten 2002].

Section 139b

1. Any person who, with the intention of eavesdropping on or recording a conversation taking place elsewhere than in a dwelling or enclosed room or premises, by means of a technical device, surreptitiously:

1°. eavesdrops on that conversation without having been instructed to do so by a participant in that conversation;
2°. records that conversation without being a participant in it and without having been instructed to do so by such a participant;

shall be liable to a term of imprisonment not exceeding three months or a fine of the third category.

2. Section 139a(2)(1°) and (3°) shall apply mutatis mutandis.

Section 139c

1. Any person who intentionally and unlawfully intercepts or records by means of a technical device data which is not intended for him and is processed or transferred by means of telecommunication or by means of a computerised device or system, shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category.

2. Subsection (1) shall not apply to intercepting or recording:

1°. data received via a radio receiver, unless a special effort was made or a prohibited receiver was used to enable such reception;
2°. by or on the instructions of the person entitled to use the telecommunication connection, except in cases of obvious misuse;
3°. for the purpose of a good operation of a public telecommunication network, for the purpose of criminal proceedings, or for the purpose of implementation of the Intelligence and Security Services Act 2002.

Section 139d

1. Any person who has a technical device installed in a particular place with the intention of unlawfully using it to eavesdrop on, intercept or record a conversation, telecommunications or other type of data transfer or data processing by a computerised device or system shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category.

2. Any person who:

a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or
b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof;

with the intention of using it in the commission of a serious offence, as referred to in section 138ab(1), 138b or 139c, shall be liable to the same punishment.

3. Any person who commits the offence referred to in subsection (2) with a view to the commission of a serious offence as referred to in section 138a(2) or (3), shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category.

Section 139e

Any person who:

1°. has at his disposal an object in which, as he knows or should reasonably suspect, data has been stored that was obtained by unlawful eavesdropping on or interception or recording of a conversation, telecommunications or other type of data transfer or data processing by a computerised device or system;
2°. has obtained data by unlawfully eavesdropping on, intercepting or recording a conversation, telecommunications or other type of data transfer or data processing by means of a computerised device or system, or data which has come to his knowledge, as he knows or should reasonably suspect, as a result of such eavesdropping, interception or recording, and who intentionally discloses such data to another person;
3°.intentionally makes an object defined in (1°) available to another person;

shall be liable to a term of imprisonment not exceeding six months or a fine of the fourth category.

Section 139f

Any person who:

1°. intentionally and unlawfully produces an image of a person who is present in a home or another place that is not open to the public by means of a technical device which is not clearly visible or notified;
2°. has at his disposal an image which, as he knows or should reasonably suspect, has been obtained by means of or as a result of the activity punishable under subsection (1°);

shall be liable to a term of imprisonment not exceeding six months or a fine of the fourth category.

Section 139g

Any person who makes public an image as referred to in the preceding section under (2°), shall be liable to a term of imprisonment not exceeding six months or a fine of the fourth category.

(…)

Part VII. Serious Offences Endangering the General Safety of Persons or Property

(…)

Section 161sexies

1. Any person who intentionally destroys, damages or renders unusable any computerised device or system infrastructure facility or any telecommunication infrastructure facility, causes the defective functioning or operation of such facility, or frustrates a safety measure taken in respect of such facility, shall be liable to:

1°. a term of imprisonment not exceeding one year or a fine of the fifth category, if such act unlawfully interferes with or disrupts the storage, processing or transfer of data for the use of the general public or causes the defective functioning of a public telecommunication network or the provision of a public telecommunication service;
2°. a term of imprisonment not exceeding six years or a fine of the fifth category, if such act is likely to generally endanger property or the provision of services;
3°. a term of imprisonment not exceeding nine years or a fine of the fifth category, if such act is likely to endanger the life of another person;
4°. a term of imprisonment not exceeding fifteen years or a fine of the fifth category, if such act is likely to endanger the life of another person and the offence results in the death of a person.

2. Any person who:

a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or
b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof;

with the intention of using it in the commission of a serious offence, as referred to in subsection (1), shall be liable to a term of imprisonment not exceeding one year or a fine of the fifth category.

Section 161septies

Any person who, through negligence, causes any computerised device or system infrastructure facility or any telecommunication infrastructure facility to be destroyed, damaged or rendered unusable, which results in the defective functioning or operation of such facility, or causes a safety measure taken in respect of such facility to be frustrated, shall be liable to:

1°. a term of imprisonment not exceeding six months or a fine of the fourth category, if such act interferes with or disrupts the storage, processing or transfer of data for the use of the general public or causes the defective functioning of a public telecommunication network or the provision of a public telecommunication service or generally endangers property or the provision of services;
2°. a term of imprisonment not exceeding one year or a fine of the fourth category, if such act endangers the life of another person;
3°. a term of imprisonment not exceeding two years or a fine of the fourth category, if the offence results in the death of a person.

(…)

Part XXII. Theft and Theft of Natural Objects

Section 310

Any person who takes any property belonging in whole or in part to another person with the intention of unlawfully appropriating it, shall be guilty of theft and shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category.

(…)

Part XXIII. Extortion and Blackmail

Section 317

1. Any person who, with the intention of benefitting himself or another unlawfully, compels a person by an act of violence or by threat of violence, to surrender any property belonging in whole or in part to that person or to a third party, or to incur a debt or relinquish a claim to a debt, or to make available data, shall be guilty of extortion and shall be liable to a term of imprisonment not exceeding nine years or a fine of the fifth category.

2. Any person who exercises the coercion, referred to in subsection (1), by threatening that data stored by means of a computerised device or system will be rendered unusable or will be disabled, or erased, shall be liable to the same punishment.

3. The provisions of section 312(2) and (3) shall apply to this serious offence.

Section 318

1. Any person who, with the intention of benefitting himself or another unlawfully, compels a person by threatening him with slander, libel or disclosure, to surrender any property belonging in whole or in part to that person or to a third party, or to incur a debt or relinquish a claim to a debt, or to make available data, shall be guilty of blackmail and shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category.

2. If an offence is committed with the intention of preparing or facilitating a terrorist offence, the term of imprisonment prescribed for the offence shall be increased by one third.

3. This serious offence shall be prosecuted only on complaint by the person against whom it was committed.

(…)

Part XXV. Deception

Section 326

1. Any person who, with the intention of benefitting himself or another person unlawfully, either by assuming a false name or a false capacity, or by cunning manoeuvres, or by a tissue of lies, induces a person to hand over any property, to render a service, to make available data, to incur a debt or relinquish a claim, shall be guilty of fraud and shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category.

2. If the offence is committed with the intention of preparing or facilitating a terrorist offence, the term of imprisonment prescribed for the offence shall be increased by one third.

Section 326b

Any person who:

1°. falsely places any name or any mark, or falsifies the authentic name or the authentic mark on or in a work of literature, science, art or craft, with the intention of making it appear as if that work had been created by the person whose name or mark he has placed on or in it;
2°. intentionally sells, offers for sale, delivers, has in store for the purpose of sale or imports into the Kingdom in Europe, a work of literature, science, art or craft, on which or in which any name or any mark has been falsely placed, or on or in which the authentic name or the authentic mark has been falsified, as if that work had been created by the person whose name or mark has been falsely placed on or in it;

shall be liable to a term of imprisonment not exceeding two years or a fine of the fifth category.

Section 326c

1. Any person who, with the intention of not paying for it in full, by technological means or by means of false signals, uses a service offered to the general public by means of telecommunication, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category.

2. Any person who intentionally:

a. openly offers for distribution,
b. has in his possession for distribution or with a view to importing such into the Netherlands, or
c. in pursuit of profit, manufactures or keeps,

an object or data clearly intended to be used in the commission of the serious offence defined in subsection (1), shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category.

3. Any person who commits the serious offences referred to in subsection (2) as a profession or business, shall be liable to either a term of imprisonment not exceeding four years and a fine of the fifth category or one of these punishments.

(…)

Part XXVII. Destruction or Damage

Section 350

1. Any person who intentionally and unlawfully destroys, damages, renders unusable or disposes of any property belonging in whole or in part to another, shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category.

2. Any person who intentionally and unlawfully kills, maims, renders unusable or disposes of an animal belonging in whole or in part to another, shall be liable to a term of imprisonment not exceeding three years of a fine of the fourth category.

Section 350a

1. Any person who intentionally and unlawfully alters, erases, renders unusable or disables data stored, processed or transferred by means of a computerised device or system or by means of telecommunication, or adds other data thereto, shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category.

2. Any person who commits the offence defined in subsection (1) after having unlawfully gained access, through a public telecommunication network, to a computerised device or system, and causes serious damage to such data, shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category.

3. Any person who intentionally and unlawfully makes available or disseminates data that is intended to cause damage in a computerised device or system, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category.

4. Any person who commits the offence defined in subsection (3) with the intention of limiting the damage resulting from such data shall not be criminally liable.

Section 350b

1. Any person who, through negligence, causes data stored, processed or transferred by means of a computerised device or system to be altered, erased, rendered unusable or disabled, or causes other data to be added thereto, shall, if this causes serious damage to that data, be liable to a term of imprisonment or of detention not exceeding one month or a fine of the second category.

2. Any person who, through negligence, causes data intended to cause damage to a computerised device or system to be unlawfully made available or disseminated, shall be liable to a term of imprisonment or detention not exceeding one month or a fine of the second category.

Section 351

Any person who intentionally and unlawfully destroys, damages, renders unusable or defective, or disposes of any railroad, electricity, computerised device or system or telecommunication infrastructure facilities or water defence, water disposal, gas or water pipeline or sewerage infrastructure facilities intended for the use of the general public, as well as any property or infrastructure facilities for the purpose of national defence, shall be liable to a term of imprisonment not exceeding three years or a fine of the fourth category.

Section 351bis

Any person who, through negligence, causes any of the property or the infrastructure facilities defined in the preceding section to be destroyed, damaged, rendered unusable or defective, or disposed of, shall be liable to a term of detention not exceeding one month or a fine of the second category.

(…)

GENERAL FINAL PROVISION

Article 479

The coming into effect of this Code shall be further regulated by the law.

We hereby ordain and command that this Act shall be published in the *Bulletin of Acts and Decrees* and that all Ministerial Departments, Authorities, Executive Bodies and Civil Servants to whom this shall be of concern, shall see to its careful enforcement.

Given at The Hague, the 3rd of March 1881

WILLEM.

The Minister of Justice,
A. E. J. MODDERMAN

Issued the fifth of March 1881.

The Minister of Justice,
A. E. J. MODDERMAN

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)

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.

[1] OJ C 365 E, 19.12.2000, p. 223.
[2] OJ C 123, 25.4.2001, p. 53.
[3] Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.
[4] OJ L 281, 23.11.1995, p. 31.
[5] OJ L 24, 30.1.1998, p. 1.

(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 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 tourist 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 trace 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 unpaid 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) [1] 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 [2] 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 harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, 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.

[1] OJ L 178, 17.7.2000, p. 1.

[2] OJ L 91, 7.4.1999, p. 10.

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 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [1] 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, 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;

(e) 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(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.

[1] OJ L 108, 24.4.2002, p. 33.

Article 3

Services concerned

1. 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.

2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4

Security

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.

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.

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 use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

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/her 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.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

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 be 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 systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers 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 when they are collected 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, free of charge, unsolicited communications for 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 concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, 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.

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 [1].

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 [2].

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.

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 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.

[1] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[2] OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

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. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

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*.

Article 21

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 12 July 2002.

For the European Parliament	*For the Council*
The President	*The President*
P. COX	T. PEDERSEN

I

(Acts whose publication is obligatory)

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)

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.

---

(1) OJ C 30, 5.2.1999, p. 4.
(2) OJ C 169, 16.6.1999, p. 36.
(3) Opinion of the European Parliament of 6 May 1999 (OJ C 279, 1.10.1999, p. 389), Council common position of 28 February 2000 (OJ C 128, 8.5.2000, p. 32) and Decision of the European Parliament of 4 May 2000 (not yet published in the Official Journal).
(4) OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

(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 [1] and 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 [2] form a vital element for protecting consumers in contractual matters; those Directives also apply in their entirety to information society services; that same Community acquis, which is fully applicable to information society services, also embraces in particular Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising [3], Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit [4], Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field [5], Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours [6], Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer production in the indication of prices of products offered to consumers [7], Council Directive 92/59/EEC of 29 June 1992 on general product safety [8], 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 on contracts relating to the purchase of the right to use immovable properties on a timeshare basis [9], Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests [10], Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions concerning liability for defective products [11], 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 [12], the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services and Council Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products [13]; this Directive

(1) OJ L 95, 21.4.1993, p. 29.
(2) OJ L 144, 4.6.1999, p. 19.
(3) OJ L 250, 19.9.1984, p. 17. Directive as amended by Directive 97/55/EC of the European Parliament and of the Council (OJ L 290, 23.10.1997, p. 18).
(4) OJ L 42, 12.2.1987, p. 48. Directive as last amended by Directive 98/7/EC of the European Parliament and of the Council (OJ L 101, 1.4.1998, p. 17).
(5) OJ L 141, 11.6.1993, p. 27. Directive as last amended by Directive 97/9/EC of the European Parliament and of the Council (OJ L 84, 26.3.1997, p. 22).
(6) OJ L 158, 23.6.1990, p. 59.
(7) OJ L 80, 18.3.1998, p. 27.
(8) OJ L 228, 11.8.1992, p. 24.
(9) OJ L 280, 29.10.1994, p. 83.
(10) OJ L 166, 11.6.1998, p. 51. Directive as amended by Directive 1999/44/EC (OJ L 171, 7.7.1999, p. 12).
(11) OJ L 210, 7.8.1985, p. 29. Directive as amended by Directive 1999/34/EC (OJ L 141, 4.6.1999, p. 20).
(12) OJ L 171, 7.7.1999, p. 12.
(13) OJ L 113, 30.4.1992, p. 13.

should be without prejudice to Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products [1] adopted within the framework of the internal market, or to directives on the protection of public health; this Directive complements information requirements established by the abovementioned Directives and in particular Directive 97/7/EC.

(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 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 form 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 individuals with regard to the processing of personal data and on the free movement of such data [2] 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 [3] 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 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 [4] 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 [5]; 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, 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 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

(1) OJ L 213, 30.7.1998, p. 9.
(2) OJ L 281, 23.11.1995, p. 31.
(3) OJ L 24, 30.1.1998, p. 1.
(4) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).
(5) OJ L 320, 28.11.1998, p. 54.

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 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 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 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.

(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 concerning the 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 [1] 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 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 communities 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 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 [2]; 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.

[1] OJ L 15, 21.1.1998, p. 14.

[2] OJ L 13, 19.1.2000, p. 12.

(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 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; 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 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 can benefit 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 as they do not alter 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.

(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 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 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 makes it necessary to guarantee victims effective 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 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 the 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 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 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 [1], 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,

HAVE 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(2) of Directive 98/34/EC as amended by Directive 98/48/EC;

[1] OJ C 23, 28.1.1999, p. 1.

(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;

(g) 'regulated profession': any profession within the meaning of either Article 1(d) of Council Directive 89/48/EEC of 21 December 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration [1] or of Article 1(f) of Council Directive 92/51/EEC of 18 June 1992 on a second general system for the recognition of professional education and training to supplement Directive 89/48/EEC [2];

(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,

[1] OJ L 19, 24.1.1989, p. 16.
[2] OJ L 209, 24.7.1992, p. 25. Directive as last amended by Commission Directive 97/38/EC (OJ L 184, 12.7.1997, p. 31).

— 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 [1].

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 [2].

(1) OJ L 117, 7.5.1997, p. 15.
(2) OJ L 145, 13.6.1977, p. 1. Directive as last amended by Directive 1999/85/EC (OJ L 277, 28.10.1999, p. 34).

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 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.

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:

'11. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects on information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).'

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 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	*For the Council*
The President	*The President*
N. FONTAINE	G. d'OLIVEIRA MARTINS

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 87/54/EEC [1] and Directive 96/9/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],

— Article 44(2) of Directive 85/611/EEC [4],

— Article 30 and Title IV of Directive 92/49/EEC [5], Title IV of Directive 92/96/EEC [6], Articles 7 and 8 of Directive 88/357/EEC [7] and Article 4 of Directive 90/619/EEC [8],

— the freedom of the parties to choose the law applicable to their contract,

— contractual obligations concerning consumer contacts,

— formal validity of contracts creating or transferring rights in real estate where such contracts are subject to mandatory formal requirements of the law of the Member State where the real estate is situated,

— the permissibility of unsolicited commercial communications by electronic mail.

---

[1] OJ L 24, 27.1.1987, p. 36.
[2] OJ L 77, 27.3.1996, p. 20.
[3] Not yet published in the Official Journal.
[4] OJ L 375, 31.12.1985, p. 3. Directive as last amended by Directive 95/26/EC (OJ L 168, 18.7.1995, p. 7).
[5] OJ L 228, 11.8.1992, p. 1. Directive as last amended by Directive 95/26/EC.
[6] OJ L 360, 9.12.1992, p. 2. Directive as last amended by Directive 95/26/EC.
[7] OJ L 172, 4.7.1988, p. 1. Directive as last amended by Directive 92/49/EC.
[8] OJ L 330, 29.11.1990, p. 50. Directive as last amended by Directive 92/96/EC.

DIRECTIVE 2006/123/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 December 2006

on services in the internal market

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular the first and third sentence of Article 47(2) and Article 55 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 Committee of the Regions [2],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [3],

Whereas:

(1) The European Community is seeking to forge ever closer links between the States and peoples of Europe and 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 movement of services is ensured. In accordance with Article 43 of the Treaty the freedom of establishment is ensured. Article 49 of the Treaty establishes the right to provide services within the Community. The elimination of barriers to the development of service activities between Member States is essential in order to strengthen the integration of the peoples of Europe and to promote balanced and sustainable economic and social progress. In eliminating such barriers it is essential to ensure that the development of service activities contributes to the fulfilment of the task laid down in Article 2 of the Treaty of promoting throughout the Community a harmonious, balanced and sustainable development of economic activities, a high level of employment and of social protection, equality between men and women, sustainable and non-inflationary growth, a high degree of competitiveness and convergence of economic performance, a high level of protection and improvement of the quality of the environment, the raising of the standard of living and quality of life and economic and social cohesion and solidarity among Member States.

(2) A competitive market in services is essential in order to promote economic growth and create jobs in the European Union. At present numerous barriers within the internal market prevent providers, particularly small and medium-sized enterprises (SMEs), from extending their operations beyond their national borders and from taking full advantage of the internal market. This weakens the worldwide competitiveness of European Union providers. A free market which compels the Member States to eliminate restrictions on cross-border provision of services while at the same time increasing transparency and information for consumers would give consumers wider choice and better services at lower prices.

(3) The report from the Commission on 'The State of the Internal Market for Services' drew up an inventory of a large number of barriers which are preventing or slowing down the development of services between Member States, in particular those provided by SMEs, which are predominant in the field of services. The report concludes that a decade after the envisaged completion of the internal market, there is still a huge gap between the vision of an integrated European Union economy and the reality as experienced by European citizens and providers. The barriers affect a wide variety of service activities across all stages of the provider's activity and have a number of common features, including the fact that they often arise from administrative burdens, the legal uncertainty associated with cross-border activity and the lack of mutual trust between Member States.

(4) Since services constitute the engine of economic growth and account for 70 % of GDP and employment in most Member States, this fragmentation of the internal market has a negative impact on the entire European economy, in particular on the competitiveness of SMEs and the movement of workers, and prevents consumers from gaining access to a greater variety of competitively priced services. It is important to point out that the services sector is a key employment sector for women in particular, and that they therefore stand to benefit greatly from new opportunities offered by the completion of the internal market for services. The European Parliament and the Council have emphasised that the removal of legal barriers to the establishment of a genuine internal market is a matter of priority for achieving the goal set by the European Council in Lisbon of 23 and 24 March 2000

[1] OJ C 221, 8.9.2005, p. 113.

[2] OJ C 43, 18.2.2005, p. 18.

[3] Opinion of the European Parliament of 16 February 2006 (not yet published in the Official Journal), Council Common Position of 24 July 2006 (OJ C 270 E, 7.11.2006, p. 1) and Position of the European Parliament of 15 November 2006. Council Decision of 11 December 2006.

of improving employment and social cohesion and achieving sustainable economic growth so as to make the European Union the most competitive and dynamic knowledge-based economy in the world by 2010, with more and better jobs. Removing those barriers, while ensuring an advanced European social model, is thus a basic condition for overcoming the difficulties encountered in implementing the Lisbon Strategy and for reviving the European economy, particularly in terms of employment and investment. It is therefore important to achieve an internal market for services, with the right balance between market opening and preserving public services and social and consumer rights.

(5) It is therefore necessary to remove barriers to the freedom of establishment for providers in Member States and barriers to the free movement of services as between Member States and to guarantee recipients and providers the legal certainty necessary for the exercise in practice of those two fundamental freedoms of the Treaty. Since the barriers in the internal market for services affect operators who wish to become established in other Member States as well as those who provide a service in another Member State without being established there, it is necessary to enable providers to develop their service activities within the internal market either by becoming established in a Member State or by making use of the free movement of services. Providers should be able to choose between those two freedoms, depending on their strategy for growth in each Member State.

(6) Those barriers cannot be removed solely by relying on direct application of Articles 43 and 49 of the Treaty, since, on the one hand, addressing them on a case-by-case basis through infringement procedures against the Member States concerned would, especially following enlargement, be extremely complicated for national and Community institutions, and, on the other hand, the lifting of many barriers requires prior coordination of national legal schemes, including the setting up of administrative cooperation. As the European Parliament and the Council have recognised, a Community legislative instrument makes it possible to achieve a genuine internal market for services.

(7) This Directive establishes a general legal framework which benefits a wide variety of services while taking into account the distinctive features of each type of activity or profession and its system of regulation. That framework is based on a dynamic and selective approach consisting in the removal, as a matter of priority, of barriers which may be dismantled quickly and, for the others, the launching of a process of evaluation, consultation and complementary harmonisation of specific issues, which will make possible the progressive and coordinated modernisation of national regulatory systems for service activities which is vital in order to achieve a genuine internal market for services by 2010. Provision should be made for a balanced mix of measures involving targeted harmonisation, administrative cooperation, the provision on the freedom to provide services and encouragement of the development of codes of conduct on certain issues. That coordination of national legislative regimes should ensure a high degree of Community legal integration and a high level of protection of general interest objectives, especially protection of consumers, which is vital in order to establish trust between Member States. This Directive also takes into account other general interest objectives, including the protection of the environment, public security and public health as well as the need to comply with labour law.

(8) It is appropriate that the provisions of this Directive concerning the freedom of establishment and the free movement of services should apply only to the extent that the activities in question are open to competition, so that they do not oblige Member States either to liberalise services of general economic interest or to privatise public entities which provide such services or to abolish existing monopolies for other activities or certain distribution services.

(9) This Directive applies only to requirements which affect the access to, or the exercise of, a service activity. Therefore, it does not apply to requirements, such as road traffic rules, rules concerning the development or use of land, town and country planning, building standards as well as administrative penalties imposed for non-compliance with such rules which do not specifically regulate or specifically affect the service activity but have to be respected by providers in the course of carrying out their economic activity in the same way as by individuals acting in their private capacity.

(10) This Directive does not concern requirements governing access to public funds for certain providers. Such requirements include notably those laying down conditions under which providers are entitled to receive public funding, including specific contractual conditions, and in particular quality standards which need to be observed as a condition for receiving public funds, for example for social services.

(11) This Directive does not interfere with measures taken by Member States, in accordance with Community law, in relation to the protection or promotion of cultural and linguistic diversity and media pluralism, including the funding thereof. This Directive does not prevent Member States from applying their fundamental rules and principles relating to the freedom of press and freedom of expression. This Directive does not affect Member State laws prohibiting discrimination on grounds of nationality or on grounds such as those set out in Article 13 of the Treaty.

(12) This Directive aims at creating a legal framework to ensure the freedom of establishment and the free movement of services between the Member States and does not harmonise or prejudice criminal law. However, Member States should not be able to restrict the freedom to provide services by applying criminal law provisions which specifically affect the access to or the exercise of a service activity in circumvention of the rules laid down in this Directive.

(13) It is equally important that this Directive fully respect Community initiatives based on Article 137 of the Treaty with a view to achieving the objectives of Article 136 thereof concerning the promotion of employment and improved living and working conditions.

(14) This Directive does not affect terms and conditions of employment, including maximum work periods and minimum rest periods, minimum paid annual holidays, minimum rates of pay as well as health, safety and hygiene at work, which Member States apply in compliance with Community law, nor does it affect relations between social partners, including the right to negotiate and conclude collective agreements, the right to strike and to take industrial action in accordance with national law and practices which respect Community law, nor does it apply to services provided by temporary work agencies. This Directive does not affect Member States' social security legislation.

(15) This Directive respects the exercise of fundamental rights applicable in the Member States and as recognised in the Charter of fundamental Rights of the European Union and the accompanying explanations, reconciling them with the fundamental freedoms laid down in Articles 43 and 49 of the Treaty. Those fundamental rights include the right to take industrial action in accordance with national law and practices which respect Community law.

(16) This Directive concerns only providers established in a Member State and does not cover external aspects. It does not concern negotiations within international organisations on trade in services, in particular in the framework of the General Agreement on Trade in Services (GATS).

(17) This Directive covers only services which are performed for an economic consideration. Services of general interest are not covered by the definition in Article 50 of the Treaty and therefore do not fall within the scope of this Directive. Services of general economic interest are services that are performed for an economic consideration and therefore do fall within the scope of this Directive. However, certain services of general economic interest, such as those that may exist in the field of transport, are excluded from the scope of this Directive and certain other services of general economic interest, for example, those that may exist in the area of postal services, are the subject of a derogation from the provision on the freedom to provide services set out in this Directive. This Directive does not deal with the funding of services of general economic interest and does not apply to systems of aids granted by Member States, in particular in the social field, in accordance with Community rules on competition. This Directive does not deal with the follow-up to the Commission White Paper on Services of General Interest.

(18) Financial services should be excluded from the scope of this Directive since these activities are the subject of specific Community legislation aimed, as is this Directive, at achieving a genuine internal market for services. Consequently, t his exclusion should cover all financial services such as banking, credit, insurance, including reinsurance, occupational or personal pensions, securities, investment funds, payments and investment advice, including the services listed in Annex I to Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions ([1]).

(19) In view of the adoption in 2002 of a package of legislative instruments relating to electronic communications networks and services, as well as to associated resources and services, which has established a regulatory framework facilitating access to those activities within the internal market, notably through the elimination of most individual authorisation schemes, it is necessary to exclude issues dealt with by those instruments from the scope of this Directive.

(20) The exclusion from the scope of this Directive as regards matters of electronic communications services as covered by Directives 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) ([2]), 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) ([3]), 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

([1]) OJ L 177, 30.6.2006, p. 1.
([2]) OJ L 108, 24.4.2002, p. 7.
([3]) OJ L 108, 24.4.2002, p. 21.

services (Framework Directive) ([1]), 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) ([2]) and 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) ([3]) should apply not only to questions specifically dealt with in these Directives but also to matters for which the Directives explicitly leave to Member States the possibility of adopting certain measures at national level.

(21) Transport services, including urban transport, taxis and ambulances as well as port services, should be excluded from the scope of this Directive.

(22) The exclusion of healthcare from the scope of this Directive should cover healthcare and pharmaceutical services provided by health professionals to patients to assess, maintain or restore their state of health where those activities are reserved to a regulated health profession in the Member State in which the services are provided.

(23) This Directive does not affect the reimbursement of healthcare provided in a Member State other than that in which the recipient of the care is resident. This issue has been addressed by the Court of Justice on numerous occasions, and the Court has recognised patients' rights. It is important to address this issue in another Community legal instrument in order to achieve greater legal certainty and clarity to the extent that this issue is not already addressed in Council Regulation (EEC) No 1408/71 of 14 June 1971 on the application of social security schemes to employed persons, to self-employed persons and to members of their families moving within the Community ([4]).

(24) Audiovisual services, whatever their mode of transmission, including within cinemas, should also be excluded from the scope of this Directive. Furthermore, this Directive should not apply to aids granted by Member States in the audiovisual sector which are covered by Community rules on competition.

(25) Gambling activities, including lottery and betting transactions, should be excluded from the scope of this Directive in view of the specific nature of these activities, which entail implementation by Member States of policies relating to public policy and consumer protection.

(26) This Directive is without prejudice to the application of Article 45 of the Treaty.

(27) This Directive should not cover those social services in the areas of housing, childcare and support to families and persons in need which are provided by the State at national, regional or local level by providers m andated by the State or by charities recognised as such by the State with the objective of ensuring support for those who are permanently or temporarily in a particular state of need because of their insufficient family income or total or partial lack of independence and for those who risk being marginalised. These services are essential in order to guarantee the fundamental right to human dignity and integrity and are a manifestation of the principles of social cohesion and solidarity and should not be affected by this Directive.

(28) This Directive does not deal with the funding of, or the system of aids linked to, social services. Nor does it affect the criteria or conditions set by Member States to ensure that social services effectively carry out a function to the benefit of the public interest and social cohesion. In addition, this Directive should not affect the principle of universal service in Member States' social services.

(29) Given that the Treaty provides specific legal bases for taxation matters and given the Community instruments already adopted in that field, it is necessary to exclude the field of taxation from the scope of this Directive.

(30) There is already a considerable body of Community law on service activities. This Directive builds on, and thus complements, the Community acquis. Conflicts between this Directive and other Community instruments have been identified and are addressed by this Directive, including by means of derogations. However, it is necessary to provide a rule for any residual and exceptional cases where there is a conflict between a provision of this Directive and a provision of another Community instrument. The existence of such a conflict should be determined in compliance with the rules of the Treaty on the right of establishment and the free movement of services.

([1]) OJ L 108, 24.4.2002, p. 33.

([2]) OJ L 108, 24.4.2002, p. 51.

([3]) OJ L 201, 31.7.2002, p. 37. Directive as amended by Directive 2006/24/EC (OJ L 105, 13.4.2006, p. 54).

([4]) OJ L 149, 5.7.1971, p. 2. Regulation as last amended by Regulation (EC) No 629/2006 of the European Parliament and of the Council (OJ L 114, 27.4.2006, p. 1).

(31) This Directive is consistent with and does not affect Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications ([1]). It deals with questions other than those relating to professional qualifications, for example professional liability insurance, commercial communications, multidisciplinary activities and administrative simplification. With regard to temporary cross-border service provision, a derogation from the provision on the freedom to provide services in this Directive ensures that Title II on the free provision of services of Directive 2005/36/EC is not affected. Therefore, none of the measures applicable under that Directive in the Member State where the service is provided is affected by the provision on the freedom to provide services.

(32) This Directive is consistent with Community legislation on consumer protection, such as 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 (the Unfair Commercial Practices Directive) ([2]) and 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) ([3]).

(33) The services covered by this Directive concern a wide variety of ever-changing activities, including business services such as management consultancy, certification and testing; facilities management, including office maintenance; advertising; recruitment services; and the services of commercial agents. The services covered are also services provided both to businesses and to consumers, such as legal or fiscal advice; real estate services such as estate agencies; construction, including the services of architects; distributive trades; the organisation of trade fairs; car rental; and travel agencies. Consumer services are also covered, such as those in the field of tourism, including tour guides; leisure services, sports centres and amusement parks; and, to the extent that they are not excluded from the scope of application of the Directive, household support services, such as help for the elderly. Those activities may involve services requiring the proximity of provider and recipient, services requiring travel by the recipient or the provider and services which may be provided at a distance, including via the Internet.

([1]) OJ L 255, 30.9.2005, p. 22.

([2]) OJ L 149, 11.6.2005, p. 22.

([3]) OJ L 364, 9.12.2004, p. 1. Regulation as amended by Directive 2005/29/EC.

(34) According to the case-law of the Court of Justice, the assessment of whether certain activities, in particular activities which are publicly funded or provided by public entities, constitute a 'service' has to be carried out on a case by case basis in the light of all their characteristics, in particular the way they are provided, organised and financed in the Member State concerned. The Court of Justice has held that the essential characteristic of remuneration lies in the fact that it constitutes consideration for the services in question and has recognised that the characteristic of remuneration is absent in the case of activities performed, for no consideration, by the State or on behalf of the State in the context of its duties in the social, cultural, educational and judicial fields, such as courses provided under the national education system, or the management of social security schemes which do not engage in economic activity. The payment of a fee by recipients, for example, a tuition or enrolment fee paid by students in order to make a certain contribution to the operating expenses of a system, does not in itself constitute remuneration because the service is still essentially financed by public funds. These activities are, therefore, not covered by the definition of service in Article 50 of the Treaty and do not therefore fall within the scope of this Directive.

(35) Non-profit making amateur sporting activities are of considerable social importance. They often pursue wholly social or recreational objectives. Thus, they might not constitute economic activities within the meaning of Community law and should fall outside the scope of this Directive.

(36) The concept of 'provider' should cover any natural person who is a national of a Member State or any legal person engaged in a service activity in a Member State, in exercise either of the freedom of establishment or of the free movement of services. The concept of provider should thus not be limited solely to cross-border service provision within the framework of the free movement of services but should also cover cases in which an operator establishes itself in a Member State in order to develop its service activities there. On the other hand, the concept of a provider should not cover the case of branches in a Member State of companies from third countries because, under Article 48 of the Treaty, the freedom of establishment and free movement of services may benefit only companies constituted in accordance with the laws of a Member State and having their registered office, central administration or principal place of business within the Community. The concept of 'recipient' should also cover third country nationals who already benefit from rights conferred upon them by Community acts such as Regulation (EEC) No 1408/71, Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents ([4]), Council Regulation (EC) No 859/2003 of 14 May 2003

([4]) OJ L 16, 23.1.2004, p. 44.

extending the provisions of Regulation (EEC) No 1408/71 and Regulation (EEC) No 574/72 to nationals of third countries who are not already covered by those provisions solely on the ground of their nationality [1] and Directive 2004/38/ECof the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States [2]. Furthermore, Member States may extend the concept of recipient to other third country nationals that are present within their territory.

(37) The place at which a provider is established should be determined in accordance 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 may also be fulfilled where a company is constituted for a given period or where it rents the building or installation through which it pursues its activity. It may also be fulfilled where a Member State grants authorisations for a limited duration only in relation to particular services. An establishment does not need to take the form of a subsidiary, branch or agency, but may consist of an office managed by a provider's own staff or by a person who is independent but authorised to act on a permanent basis for the undertaking, as would be the case with an agency. According to this definition, which requires the actual pursuit of an economic activity at the place of establishment of the provider, a mere letter box does not constitute an establishment. Where a provider has several places of establishment, it is important to determine the place of establishment from which the actual service concerned is provided. Where it is difficult to determine from which of several places of establishment a given service is provided, the location of the provider's centre of activities relating to this particular service should be that place of establishment.

(38) The concept of 'legal persons', according to the Treaty provisions 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 Treaty, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

(39) The concept of 'authorisation scheme' should cover, inter alia, the administrative procedures for granting authorisations, licences, approvals or concessions, and also the obligation, in order to be eligible to exercise the activity, to be registered as a member of a profession or entered in a register, roll or database, to be officially appointed to a body or to obtain a card attesting to membership of a particular profession. Authorisation may be granted not only by a formal decision but also by an implicit decision arising, for example, from the silence of the competent authority or from the fact that the interested party must await acknowledgement of receipt of a declaration in order to commence the activity in question or for the latter to become lawful.

(40) The concept of 'overriding reasons relating to the public interest' to which reference is made in certain provisions of this Directive has been developed by the Court of Justice in its case law in relation to Articles 43 and 49 of the Treaty and may continue to evolve. The notion as recognised in the case law of the Court of Justice covers at least the following grounds: public policy, public security and public health, within the meaning of Articles 46 and 55 of the Treaty; the maintenance of order in society; social policy objectives; the protection of the recipients of services; consumer protection; the protection of workers, including the social protection of workers; animal welfare; the preservation of the financial balance of the social security system; the prevention of fraud; the prevention of unfair competition; the protection of the environment and the urban environment, including town and country planning; the protection of creditors; safeguarding the sound administration of justice; road safety; the protection of intellectual property; cultural policy objectives, including safeguarding the freedom of expression of various elements, in particular social, cultural, religious and philosophical values of society; the need to ensure a high level of education, the maintenance of press diversity and the promotion of the national language; the preservation of national historical and artistic heritage; and veterinary policy.

(41) The concept of 'public policy', as interpreted by the Court of Justice, covers the protection against a genuine and sufficiently serious threat affecting one of the fundamental interests of society and may include, in particular, issues relating to human dignity, the protection of minors and vulnerable adults and animal welfare. Similarly, the concept of public security includes issues of public safety.

(42) The rules relating to administrative procedures should not aim at harmonising administrative procedures but at removing overly burdensome authorisation schemes, procedures and formalities that hinder the freedom of establishment and the creation of new service undertakings therefrom.

[1] OJ L 124, 20.5.2003, p. 1.
[2] OJ L 158, 30.4.2004, p. 77.

(43) One of the fundamental difficulties faced, in particular by SMEs, in accessing service activities and exercising them is the complexity, length and legal uncertainty of administrative procedures. For this reason, following the example of certain modernising and good administrative practice initiatives undertaken at Community and national level, it is necessary to establish principles of administrative simplification, inter alia through the limitation of the obligation of prior authorisation to cases in which it is essential and the introduction of the principle of tacit authorisation by the competent authorities after a certain period of time elapsed. Such modernising action, while maintaining the requirements on transparency and the updating of information relating to operators, is intended to eliminate the delays, costs and dissuasive effects which arise, for example, from unnecessary or excessively complex and burdensome procedures, the duplication of procedures, the 'red tape' involved in submitting documents, the arbitrary use of powers by the competent authorities, indeterminate or excessively long periods before a response is given, the limited duration of validity of authorisations granted and disproportionate fees and penalties. Such practices have particularly significant dissuasive effects on providers wishing to develop their activities in other Member States and require coordinated modernisation within an enlarged internal market of twenty-five Member States.

(44) Member States should introduce, where appropriate, forms harmonised at Community level, as established by the Commission, which will serve as an equivalent to certificates, attestations or any other document in relation to establishment.

(45) In order to examine the need for simplifying procedures and formalities, Member States should be able, in particular, to take into account their necessity, number, possible duplication, cost, clarity and accessibility, as well as the delay and practical difficulties to which they could give rise for the provider concerned.

(46) In order to facilitate access to service activities and the exercise thereof in the internal market, it is necessary to establish an objective, common to all Member States, of administrative simplification and to lay down provisions concerning, inter alia, the right to information, procedures by electronic means and the establishment of a framework for authorisation schemes. Other measures adopted at national level to meet that objective could involve reduction of the number of procedures and formalities applicable to service activities and the restriction of such procedures and formalities to those which are essential in order to achieve a general interest objective and which do not duplicate each other in terms of content or purpose.

(47) With the aim of administrative simplification, general formal requirements, such as presentation of original documents, certified copies or a certified translation, should not be imposed, except where objectively justified by an overriding reason relating to the public interest, such as the protection of workers, public health, the protection of the environment or the protection of consumers. It is also necessary to ensure that an authorisation as a general rule permits access to, or exercise of, a service activity throughout the national territory, unless a new authorisation for each establishment, for example for each new hypermarket, or an authorisation that is restricted to a specific part of the national territory is objectively justified by an overriding reason relating to the public interest.

(48) In order to further simplify administrative procedures, it is appropriate to ensure that each provider has a single point through which he can complete all procedures and formalities (hereinafter referred to as 'points of single contact'). The number of points of single contact per Member State may vary according to regional or local competencies or according to the activities concerned. The creation of points of single contact should not interfere with the allocation of functions among competent authorities within each national system. Where several authorities at regional or local level are competent, one of them may assume the role of point of single contact and coordinator. Points of single contact may be set up not only by administrative authorities but also by chambers of commerce or crafts, or by the professional organisations or private bodies to which a Member State decides to entrust that function. Points of single contact have an important role to play in providing assistance to providers either as the authority directly competent to issue the documents necessary to access a service activity or as an intermediary between the provider and the authorities which are directly competent.

(49) The fee which may be charged by points of single contact should be proportionate to the cost of the procedures and formalities with which they deal. This should not prevent Member States from entrusting the points of single contact with the collection of other administrative fees, such as the fee of supervisory bodies.

(50) It is necessary for providers and recipients of services to have easy access to certain types of information It should be for each Member State to determine, within the framework of this Directive, the way in which providers and recipients are provided with information. In particular, the obligation on Member States to ensure that relevant information is easily accessible to providers and recipients and that it can be accessed by the public without obstacle could be fulfilled by making this information accessible through a website. Any information given should be provided in a clear and unambiguous manner.

(51) The information provided to providers and recipients of services should include, in particular, information on procedures and formalities, contact details of the competent authorities, conditions for access to public registers and data bases and information concerning available remedies and the contact details of associations and organisations from which providers or recipients can obtain practical assistance. The obligation on competent authorities to assist providers and recipients should not include the provision of legal advice in individual cases. Nevertheless, general information on the way in which requirements are usually interpreted or applied should be given. Issues such as liability for providing incorrect or misleading information should be determined by Member States.

(52) The setting up, in the reasonably near future, of electronic means of completing procedures and formalities will be vital for administrative simplification in the field of service activities, for the benefit of providers, recipients and competent authorities. In order to meet that obligation as to results, national laws and other rules applicable to services may need to be adapted. This obligation should not prevent Member States from providing other means of completing such procedures and formalities, in addition to electronic means. The fact that it must be possible to complete those procedures and formalities at a distance means, in particular, that Member States must ensure that they may be completed across borders. The obligation as to results does not cover procedures or formalities which by their very nature are impossible to complete at a distance. Furthermore, this does not interfere with Member States' legislation on the use of languages.

(53) The granting of licences for certain service activities may require an interview with the applicant by the competent authority in order to assess the applicant's personal integrity and suitability for carrying out the service in question. In such cases, the completion of formalities by electronic means may not be appropriate.

(54) The possibility of gaining access to a service activity should be made subject to authorisation by the competent authorities only if that decision satisfies the criteria of non-discrimination, necessity and proportionality. That means, in particular, that authorisation schemes should be permissible only where an a posteriori inspection would not be effective because of the impossibility of ascertaining the defects of the services concerned a posteriori, due account being taken of the risks and dangers which could arise in the absence of a prior inspection. However, the provision to that effect made by this Directive cannot be relied upon in order to justify authorisation schemes which are prohibited by other Community instruments such as Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures [1], or 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) [2]. The results of the process of mutual evaluation will make it possible to determine, at Community level, the types of activity for which authorisation schemes should be eliminated.

(55) This Directive should be without prejudice to the possibility for Member States to withdraw authorisations after they have been issued, if the conditions for the granting of the authorisation are no longer fulfilled.

(56) According to the case law of the Court of Justice, public health, consumer protection, animal health and the protection of the urban environment constitute overriding reasons relating to the public interest. Such overriding reasons may justify the application of authorisation schemes and other restrictions. However, no such authorisation scheme or restriction should discriminate on grounds of nationality. Further, the principles of necessity and proportionality should always be respected.

(57) The provisions of this Directive relating to authorisation schemes should concern cases where the access to or exercise of a service activity by operators requires a decision by a competent authority. This concerns neither decisions by competent authorities to set up a public or private entity for the provision of a particular service nor the conclusion of contracts by competent authorities for the provision of a particular service which is governed by rules on public procurement, since this Directive does not deal with rules on public procurement.

(58) In order to facilitate access to and exercise of service activities, it is important to evaluate and report on authorisation schemes and their justification. This reporting obligation concerns only the existence of authorisation schemes and not the criteria and conditions for the granting of an authorisation.

[1] OJ L 13, 19.1.2000, p. 12.
[2] OJ L 178, 17.7.2000, p. 1.

(59) The authorisation should as a general rule enable the provider to have access to the service activity, or to exercise that activity, throughout the national territory, unless a territorial limit is justified by an overriding reason relating to the public interest. For example, environmental protection may justify the requirement to obtain an individual authorisation for each installation on the national territory. This provision should not affect regional or local competences for the granting of authorisations within the Member States.

(60) This Directive, and in particular the provisions concerning authorisation schemes and the territorial scope of an authorisation, should not interfere with the division of regional or local competences within the Member States, including regional and local self-government and the use of official languages.

(61) The provision relating to the non-duplication of conditions for the granting of an authorisation should not prevent Member States from applying their own conditions as specified in the authorisation scheme. It should only require that competent authorities, when considering whether these conditions are met by the applicant, take into account the equivalent conditions which have already been satisfied by the applicant in another Member State. This provision should not require the application of the conditions for the granting of an authorisation provided for in the authorisation scheme of another Member State.

(62) Where the number of authorisations available for an activity is limited because of scarcity of natural resources or technical capacity, a procedure for selection from among several potential candidates should be adopted with the aim of developing through open competition the quality and conditions for supply of services available to users. Such a procedure should provide guarantees of transparency and impartiality and the authorisation thus granted should not have an excessive duration, be subject to automatic renewal or confer any advantage on the provider whose authorisation has just expired. In particular, the duration of the authorisation granted should be fixed in such a way that it does not restrict or limit free competition beyond what is necessary in order to enable the provider to recoup the cost of investment and to make a fair return on the capital invested. This provision should not prevent Member States from limiting the number of authorisations for reasons other than scarcity of natural resources or technical capacity. These authorisationsshould remain in any case subject to the other provisions of this Directive relating to authorisation schemes.

(63) In the absence of different arrangements, failing a response within a time period, an authorisation should be deemed to have been granted. However, different arrangements may be put in place in respect of certain activities, where objectively justified by overriding reasons relating to the public interest, including a legitimate interest of third parties. Such different arrangements could include national rules according to which, in the absence of a response of the competent authority, the application is deemed to have been rejected, this rejection being open to challenge before the courts.

(64) In order to establish a genuine internal market for services, it is necessary to abolish any restrictions on the freedom of establishment and the free movement of services which are still enshrined in the laws of certain Member States and which are incompatible with Articles 43 and 49 of the Treaty respectively. The restrictions to be prohibited particularly affect the internal market for services and should be systematically dismantled as soon as possible.

(65) Freedom of establishment is predicated, in particular, upon the principle of equal treatment, which entails the prohibition not only of any discrimination on grounds of nationality but also of any indirect discrimination based on other grounds but capable of producing the same result. Thus, access to a service activity or the exercise thereof in a Member State, either as a principal or secondary activity, should not be made subject to criteria such as place of establishment, residence, domicile or principal provision of the service activity. However, these criteria should not include requirements according to which a provider or one of his employees or a representative must be present during the exercise of the activity when this is justified by an overriding reason relating to the public interest. Furthermore, a Member State should not restrict the legal capacity or the right of companies, incorporated in accordance with the law of another Member State on whose territory they have their primary establishment, to bring legal proceedings. Moreover, a Member State should not be able to confer any advantages on providers having a particular national or local socio-economic link; nor should it be able to restrict, on grounds of place of establishment, the provider's freedom to acquire, exploit or dispose of rights and goods or to access different forms of credit or accommodation in so far as those choices are useful for access to his activity or for the effective exercise thereof.

(66) Access to or the exercise of a service activity in the territory of a Member State should not be subject to an economic test. The prohibition of economic tests as a prerequisite for the grant of authorisation should cover economic tests as such, but not requirements which are objectively justified by overriding reasons relating to the public interest, such as the protection of the urban environment, social policy or public health. The prohibition should not affect the exercise of the powers of the authorities responsible for applying competition law.

(67) With respect to financial guarantees or insurance, the prohibition of requirements should concern only the obligation that the requested financial guarantees or insurance must be obtained from a financial institution established in the Member State concerned.

(68) With respect to pre-registration, the prohibition of requirements should concern only the obligation that the provider, prior to the establishment, be pre-registered for a given period in a register held in the Member State concerned.

(69) In order to coordinate the modernisation of national rules and regulations in a manner consistent with the requirements of the internal market, it is necessary to evaluate certain non-discriminatory national requirements which, by their very nature, could severely restrict or even prevent access to an activity or the exercise thereof under the freedom of establishment. This evaluation process should be limited to the compatibility of these requirements with the criteria already established by the Court of Justice on the freedom of establishment. It should not concern the application of Community competition law. Where such requirements are discriminatory or not objectively justified by an overriding reason relating to the public interest, or where they are disproportionate, they must be abolished or amended. The outcome of this assessment will be different according to the nature of the activity and the public interest concerned. In particular, such requirements could be fully justified when they pursue social policy objectives.

(70) For the purposes of this Directive, and without prejudice to Article 16 of the Treaty, services may be considered to be services of general economic interest only if they are provided in application of a special task in the public interest entrusted to the provider by the Member State concerned. This assignment should be made by way of one or more acts, the form of which is determined by the Member State concerned, and should specify the precise nature of the special task.

(71) The mutual evaluation process provided for in this Directive should not affect the freedom of Member States to set in their legislation a high level of protection of the public interest, in particular in relation to social policy objectives. Furthermore, it is necessary that the mutual evaluation process take fully into account the specificity of services of general economic interest and of the particular tasks assigned to them. This may justify certain restrictions on the freedom of establishment, in particular where such restrictions pursue the protection of public health and social policy objectives and where they satisfy the conditions set out in Article 15(3)(a), (b) and (c). For example, with regard to the obligation to take a specific legal form in order to exercise certain services in the social field, the Court of Justice has already recognised that it may be justified to subject the provider to a requirement to be non-profit making.

(72) Services of a general economic interest are entrusted with important tasks relating to social and territorial cohesion. The performance of these tasks should not be obstructed as a result of the evaluation process provided for in this Directive. Requirements which are necessary for the fulfilment of such tasks should not be affected by this process while, at the same time, unjustified restrictions on the freedom of establishment should be addressed.

(73) The requirements to be examined include national rules which, on grounds other than those relating to professional qualifications, reserve access to certain activities to particular providers. These requirements also include obligations on a provider to take a specific legal form, in particular to be a legal person, to be a company with individual ownership, to be a non-profit making organisation or a company owned exclusively by natural persons, and requirements which relate to the shareholding of a company, in particular obligations to hold a minimum amount of capital for certain service activities or to have a specific qualification in order to hold share capital in or to manage certain companies. The evaluation of the compatibility of fixed minimum and/or maximum tariffs with the freedom of establishment concerns only tariffs imposed by competent authorities specifically for the provision of certain services and not, for example, general rules on price determination, such as for the renting of houses.

(74) The mutual evaluation process means that during the transposition period Member States will first have to conduct a screening of their legislation in order to ascertain whether any of the above mentioned requirements exists in their legal systems. At the latest by the end of the transposition period, Member States should draw up a report on the results of this screening. Each report will be submitted to all other Member States and interested parties. Member States will then have six months in which to submit their observations on these reports. At the latest by one year after the date of transposition of this Directive, the Commission should draw up a summary report, accompanied where appropriate by proposals for further initiatives. If necessary the Commission, in cooperation with the Member States, could assist them to design a common method.

(75) The fact that this Directive specifies a number of requirements to be abolished or evaluated by the Member States during the transposition period is without prejudice to any infringement proceedings against a Member State for failure to fulfil its obligations under Articles 43 or 49 of the Treaty.

(76) This Directive does not concern the application of Articles 28 to 30 of the Treaty relating to the free movement of goods. The restrictions prohibited pursuant to the provision on the freedom to provide services cover the requirements applicable to access to service activities or to the exercise thereof and not those applicable to goods as such.

(77) Where an operator travels to another Member State to exercise a service activity there, a distinction should be made between situations covered by the freedom of establishment and those covered, due to the temporary nature of the activities concerned, by the free movement of services. As regards the distinction between the freedom of establishment and the free movement of services, according to the case law of the Court of Justice the key element is whether or not the operator is established in the Member State where it provides the service concerned. If the operator is established in the Member State where it provides its services, it should come under the scope of application of the freedom of establishment. If, by contrast, the operator is not established in the Member State where the service is provided, its activities should be covered by the free movement of services. The Court of Justice has consistently held that the temporary nature of the activities in question should be determined in the light not only of the duration of the provision of the service, but also of its regularity, periodical nature or continuity. The fact that the activity is temporary should not mean that the provider may not equip itself with some forms of infrastructure in the Member State where the service is provided, such as an office, chambers or consulting rooms, in so far as such infrastructure is necessary for the purposes of providing the service in question.

(78) In order to secure effective implementation of the free movement of services and to ensure that recipients and providers can benefit from and supply services throughout the Community regardless of borders, it is necessary to clarify the extent to which requirements of the Member State where the service is provided can be imposed. It is indispensable to provide that the provision on the freedom to provide services does not prevent the Member State where the service is provided from imposing, in compliance with the principles set out in Article 16(1)(a) to (c), its specific requirements for reasons of public policy or public security or for the protection of public health or the environment.

(79) The Court of Justice has consistently held that Member States retain the right to take measures in order to prevent providers from abusively taking advantage of the internal market principles. Abuse by a provider should be established on a case by case basis.

(80) It is necessary to ensure that providers are able to take equipment which is integral to the provision of their service with them when they travel to provide services in another Member State. In particular, it is important to avoid cases in which the service could not be provided without the equipment or situations in which providers incur additional costs, for example, by hiring or purchasing different equipment to that which they habitually use or by needing to deviate significantly from the way they habitually carry out their activity.

(81) The concept of equipment does not refer to physical objects which are either supplied by the provider to the client or become part of a physical object as a result of the service activity, such as building materials or spare parts, or which are consumed or left in situ in the course of the service provision, such as combustible fuels, explosives, fireworks, pesticides, poisons or medicines.

(82) The provisions of this Directive should not preclude the application by a Member State of rules on employment conditions. Rules laid down by law, regulation or administrative provisions should, in accordance with the Treaty, be justified for reasons relating to the protection of workers and be non-discriminatory, necessary, and proportionate, as interpreted by the Court of Justice, and comply with other relevant Community law.

(83) It is necessary to ensure that the provision on the freedom to provide services may be departed from only in the areas covered by derogations. Those derogations are necessary in order to take into account the level of integration of the internal market or certain Community instruments relating to services pursuant to which a provider is subject to the application of a law other than that of the Member State of establishment. Moreover, by way of exception, measures against a given provider should also be adopted in certain individual cases and under certain strict procedural and substantive conditions. In addition, any restriction of the free movement of services should be permitted, by way of exception, only if it is consistent with fundamental rights which form an integral part of the general principles of law enshrined in the Community legal order.

(84) The derogation from the provision on the freedom to provide services concerning postal services should cover both activities reserved to the universal service provider and other postal services.

(85) The derogation from the provision on the freedom to provide services relating to the judicial recovery of debts and the reference to a possible future harmonisation instrument should concern only the access to and the exercise of activities which consist, notably, in bringing actions before a court relating to the recovery of debts.

(86) This Directive should not affect terms and conditions of employment which, pursuant to Directive 96/71/ECof the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services [1], apply to workers posted to provide a service in the territory of another Member State. In such cases, Directive 96/71/EC stipulates that providers have to comply with terms and conditions of employment in a listed number of areas applicable in the Member State where the service is provided. These are: maximum work periods and minimum rest periods, minimum paid annual holidays, minimum rates of pay, including overtime rates, the conditions of hiring out of workers, in particular the protection of workers hired out by temporary employment undertakings, health, safety and hygiene at work, protective measures with regard to the terms and conditions of employment of pregnant women or women who have recently given birth and of children and young people and equality of treatment between men and women and other provisions on non-discrimination. This not only concerns terms and conditions of employment which are laid down by law but also those laid down in collective agreements or arbitration awards that are officially declared or de facto universally applicable within the meaning of Directive 96/71/EC. Moreover, this Directive should not prevent Member States from applying terms and conditions of employment on matters other than those listed in Article 3(1) of Directive 96/71/EC on the grounds of public policy.

(87) Neither should this Directive affect terms and conditions of employment in cases where the worker employed for the provision of a cross-border service is recruited in the Member State where the service is provided. Furthermore, this Directive should not affect the right for the Member State where the service is provided to determine the existence of an employment relationship and the distinction between self-employed persons and employed persons, including 'false self-employed persons'. In that respect the essential characteristic of an employment relationship within the meaning of Article 39 of the Treaty should be the fact that for a certain period of time a person provides services for and under the direction of another person in return for which he receives remuneration. Any activity which a person performs outside a relationship of subordination must be classified as an activity pursued in a self-employed capacity for the purposes of Articles 43 and 49 of the Treaty.

(88) The provision on the freedom to provide services should not apply in cases where, in conformity with Community law, an activity is reserved in a Member State to a particular profession, for example requirements which reserve the provision of legal advice to lawyers.

(89) The derogation from the provision on the freedom to provide services concerning matters relating to the registration of vehicles leased in a Member State other than that in which they are used follows from the case law of the Court of Justice, which has recognised that a Member State may impose such an obligation, in accordance with proportionate conditions, in the case of vehicles used on its territory. That exclusion does not cover occasional or temporary rental.

(90) Contractual relations between the provider and the client as well as between an employer and employee should not be subject to this Directive. The applicable law regarding the contractual or non contractual obligations of the provider should be determined by the rules of private international law.

(91) It is necessary to afford Member States the possibility, exceptionally and on a case-by-case basis, of taking measures which derogate from the provision on the freedom to provide services in respect of a provider established in another Member State on grounds of the safety of services. However, it should be possible to take such measures only in the absence of harmonisation at Community level.

(92) Restrictions on the free movement of services, contrary to this Directive, may arise not only from measures applied to providers, but also from the many barriers to the use of services by recipients, especially consumers. This Directive mentions, by way of illustration, certain types of restriction applied to a recipient wishing to use a service performed by a provider established in another Member State. This also includes cases where recipients of a service are under an obligation to obtain authorisation from or to make a declaration to their competent authorities in order to receive a service from a provider established in another Member State. This does not concern general authorisation schemes which also apply to the use of a service supplied by a provider established in the same Member State.

[1] OJ L 18, 21.1.1997, p. 1.

(93) The concept of financial assistance provided for the use of a particular service should not apply to systems of aids granted by Member States, in particular in the social field or in the cultural sector, which are covered by Community rules on competition, nor to general financial assistance not linked to the use of a particular service, for example grants or loans to students.

(94) In accordance with the Treaty rules on the free movement of services, discrimination on grounds of the nationality of the recipient or national or local residence is prohibited. Such discrimination could take the form of an obligation, imposed only on nationals of another Member State, to supply original documents, certified copies, a certificate of nationality or official translations of documents in order to benefit from a service or from more advantageous terms or prices. However, the prohibition of discriminatory requirements should not preclude the reservation of advantages, especially as regards tariffs, to certain recipients, if such reservation is based on legitimate and objective criteria.

(95) The principle of non-discrimination within the internal market means that access by a recipient, and especially by a consumer, to a service on offer to the public may not be denied or restricted by application of a criterion, included in general conditions made available to the public, relating to the recipient's nationality or place of residence. It does not follow that it will be unlawful discrimination if provision were made in such general conditions for different tariffs and conditions to apply to the provision of a service, where those tariffs, prices and conditions are justified for objective reasons that can vary from country to country, such as additional costs incurred because of the distance involved or the technical characteristics of the provision of the service, or different market conditions, such as higher or lower demand influenced by seasonality, different vacation periods in the Member States and pricing by different competitors, or extra risks linked to rules differing from those of the Member State of establishment. Neither does it follow that the non-provision of a service to a consumer for lack of the required intellectual property rights in a particular territory would constitute unlawful discrimination.

(96) It is appropriate to provide that, as one of the means by which the provider may make the information which he is obliged to supply easily accessible to the recipient, he supply his electronic address, including that of his website. Furthermore, the obligation to make available certain information in the provider's information documents which present his services in detail should not cover commercial communications of a general nature, such as advertising, but rather documents giving a detailed description of the services proposed, including documents on a website.

(97) It is necessary to provide in this Directive for certain rules on high quality of services, ensuring in particular information and transparency requirements. These rules should apply both in cases of cross border provision of services between Member States and in cases of services provided in a Member State by a provider established there, without imposing unnecessary burdens on SMEs. They should not in any way prevent Member States from applying, in conformity with this Directive and other Community law, additional or different quality requirements.

(98) Any operator providing services involving a direct and particular health, safety or financial risk for the recipient or a third person should, in principle, be covered by appropriate professional liability insurance, or by another form of guarantee which is equivalent or comparable, which means, in particular, that such an operator should as a general rule have adequate insurance cover for services provided in one or more Member States other than the Member State of establishment.

(99) The insurance or guarantee should be appropriate to the nature and extent of the risk. Therefore it should be necessary for the provider to have cross-border cover only if that provider actually provides services in other Member States. Member States should not lay down more detailed rules concerning the insurance cover and fix for example minimum thresholds for the insured sum or limits on exclusions from the insurance cover. Providers and insurance companies should maintain the necessary flexibility to negotiate insurance policies precisely targeted to the nature and extent of the risk. Furthermore, it is not necessary for an obligation of appropriate insurance to be laid down by law. It should be sufficient if an insurance obligation is part of the ethical rules laid down by professional bodies. Finally, there should be no obligation for insurance companies to provide insurance cover.

(100) It is necessary to put an end to total prohibitions on commercial communications by the regulated professions, not by removing bans on the content of a commercial communication but rather by removing those bans which, in a general way and for a given profession, forbid one or more forms of commercial communication, such as a ban on all advertising in one or more given media. As regards the content and methods of commercial communication, it is necessary to encourage professionals to draw up, in accordance with Community law, codes of conduct at Community level.

(101) It is necessary and in the interest of recipients, in particular consumers, to ensure that it is possible for providers to offer multidisciplinary services and that restrictions in this regard be limited to what is necessary to ensure the impartiality, independence and integrity of the regulated professions. This does not affect restrictions or prohibitions on carrying out particular activities which aim at ensuring independence in cases in which a Member State entrusts a provider with a particular task, notably in the area of urban development, nor should it affect the application of competition rules.

(102) In order to increase transparency and promote assessments based on comparable criteria with regard to the quality of the services offered and supplied to recipients, it is important that information on the meaning of quality labels and other distinctive marks relating to these services be easily accessible. That obligation of transparency is particularly important in areas such as tourism, especially the hotel business, in which the use of a system of classification is widespread. Moreover, it is appropriate to examine the extent to which European standardisation could facilitate compatibility and quality of services. European standards are drawn up by the European standards-setting bodies, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI). Where appropriate, the Commission may, in accordance with the procedures laid down 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 [1] and of rules on Information Society services, issue a mandate for the drawing up of specific European standards.

(103) In order to solve potential problems with compliance with judicial decisions, it is appropriate to provide that Member States recognise equivalent guarantees lodged with institutions or bodies such as banks, insurance providers or other financial services providers established in another Member State.

(104) The development of a network of Member States' consumer protection authorities, which is the subject of Regulation (EC) No 2006/2004, complements the cooperation provided for in this Directive. The application of consumer protection legislation in cross-border cases, in particular with regard to new marketing and selling practices, as well as the need to remove certain specific obstacles to cooperation in this field, necessitates a greater degree of cooperation between Member States. In particular, it is necessary in this area to ensure that Member States require the cessation of illegal practices by operators in their territory who target consumers in another Member State.

(105) Administrative cooperation is essential to make the internal market in services function properly. Lack of cooperation between Member States results in proliferation of rules applicable to providers or duplication of controls for cross-border activities, and can also be used by rogue traders to avoid supervision or to circumvent applicable national rules on services. It is, therefore, essential to provide for clear, legally binding obligations for Member States to cooperate effectively.

(106) For the purposes of the Chapter on administrative cooperation, 'supervision' should cover activities such as monitoring and fact finding, problem solving, enforcement and imposition of sanctions and subsequent follow-up activities.

(107) In normal circumstances mutual assistance should take place directly between competent authorities. The liaison points designated by Member States should be required to facilitate this process only in the event of difficulties being encountered, for instance if assistance is required to identify the relevant competent authority.

(108) Certain obligations of mutual assistance should apply to all matters covered by this Directive, including those relating to cases where a provider establishes in another Member State. Other obligations of mutual assistance should apply only in cases of cross-border provision of services, where the provision on the freedom to provide services applies. A further set of obligations should apply in all cases of cross-border provision of services, including areas not covered by the provision on the freedom to provide services. Cross-border provision of services should include cases where services are provided at a distance and where the recipient travels to the Member State of establishment of the provider in order to receive services.

(109) In cases where a provider moves temporarily to a Member State other than the Member State of establishment, it is necessary to provide for mutual assistance between those two Member States so that the former can carry out checks, inspections and enquiries at the request of the Member State of establishment or carry out such checks on its own initiative if these are merely factual checks.

(110) It should not be possible for Member States to circumvent the rules laid down in this Directive, including the provision on the freedom to provide services, by conducting checks, inspections or investigations which are discriminatory or disproportionate.

[1] OJ L 204, 21.7.1998, p. 37. Directive as last amended by the 2003 Act of Accession.

(111) The provisions of this Directive concerning exchange of information regarding the good repute of providers should not pre-empt initiatives in the area of police and judicial cooperation in criminal matters, in particular on the exchange of information between law enforcement authorities of the Member States and on criminal records.

(112) Cooperation between Member States requires a well-functioning electronic information system in order to allow competent authorities easily to identify their relevant interlocutors in other Member States and to communicate in an efficient way.

(113) It is necessary to provide that the Member States, in cooperation with the Commission, are to encourage interested parties to draw up codes of conduct at Community level, aimed, in particular, at promoting the quality of services and taking into account the specific nature of each profession. Those codes of conduct should comply with Community law, especially competition law. They should be compatible with legally binding rules governing professional ethics and conduct in the Member States.

(114) Member States should encourage the setting up of codes of conduct, in particular, by professional bodies, organisations and associations at Community level. These codes of conduct should include, as appropriate to the specific nature of each profession, rules for commercial communications relating to the regulated professions and rules of professional ethics and conduct of the regulated professions which aim, in particular, at ensuring independence, impartiality and professional secrecy. In addition, the conditions to which the activities of estate agents are subject should be included in such codes of conduct. Member States should take accompanying measures to encourage professional bodies, organisations and associations to implement at national level the codes of conduct adopted at Community level.

(115) Codes of conduct at Community level are intended to set minimum standards of conduct and are complementary to Member States' legal requirements. They do not preclude Member States, in accordance with Community law, from taking more stringent measures in law or national professional bodies from providing for greater protection in their national codes of conduct.

(116) Since the objectives of this Directive, namely the elimination of barriers to the freedom of establishment for providers in the Member States and to the free provision of services between Member States, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale 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 Directive does not go beyond what is necessary in order to achieve those objectives.

(117) The measures necessary for the implementation of this Directive 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 [1].

(118) In accordance with paragraph 34 of the Interinstitutional Agreement on better law-making [2], Member States are encouraged to draw up, for themselves and in the interest of the Community, their own tables, which will, as far as possible, illustrate the correlation between the Directive and the transposition measures, and to make them public,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive establishes general provisions facilitating the exercise of the freedom of establishment for service providers and the free movement of services, while maintaining a high quality of services.

2. This Directive does not deal with the liberalisation of services of general economic interest, reserved to public or private entities, nor with the privatisation of public entities providing services.

3. This Directive does not deal with the abolition of monopolies providing services nor with aids granted by Member States which are covered by Community rules on competition.

This Directive does not affect the freedom of Member States to define, in conformity with Community law, what they consider to be services of general economic interest, how those services should be organised and financed, in compliance with the State aid rules, and what specific obligations they should be subject to.

4. This Directive does not affect measures taken at Community level or at national level, in conformity with Community law, to protect or promote cultural or linguistic diversity or media pluralism.

[1] OJ L 184, 17.7.1999, p. 23. Decision as amended by Decision 2006/512/EC (OJ L 200, 22.7.2006, p. 11).

[2] OJ C 321, 31.12.2003, p. 1.

5. This Directive does not affect Member States' rules of criminal law. However, Member States may not restrict the freedom to provide services by applying criminal law provisions which specifically regulate or affect access to or exercise of a service activity in circumvention of the rules laid down in this Directive.

6. This Directive does not affect labour law, that is any legal or contractual provision concerning employment conditions, working conditions, including health and safety at work and the relationship between employers and workers, which Member States apply in accordance with national law which respects Community law. Equally, this Directive does not affect the social security legislation of the Member States.

7. This Directive does not affect the exercise of fundamental rights as recognised in the Member States and by Community law. Nor does it affect the right to negotiate, conclude and enforce collective agreements and to take industrial action in accordance with national law and practices which respect Community law.

Article 2

Scope

1. This Directive shall apply to services supplied by providers established in a Member State.

2. This Directive shall not apply to the following activities:

(a) non-economic services of general interest;

(b) financial services, such as banking, credit, insurance and re-insurance, occupational or personal pensions, securities, investment funds, payment and investment advice, including the services listed in Annex I to Directive 2006/48/EC;

(c) electronic communications services and networks, and associated facilities and services, with respect to matters covered by Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC and 2002/58/EC;

(d) services in the field of transport, including port services, falling within the scope of Title V of the Treaty;

(e) services of temporary work agencies;

(f) healthcare services whether or not they are provided via healthcare facilities, and regardless of the ways in which they are organised and financed at national level or whether they are public or private;

(g) audiovisual services, including cinematographic services, whatever their mode of production, distribution and transmission, and radio broadcasting;

(h) gambling activities which involve wagering a stake with pecuniary value in games of chance, including lotteries, gambling in casinos and betting transactions;

(i) activities which are connected with the exercise of official authority as set out in Article 45 of the Treaty;

(j) social services relating to social housing, childcare and support of families and persons permanently or temporarily in need which are provided by the State, by providers mandated by the State or by charities recognised as such by the State;

(k) private security services;

(l) services provided by notaries and bailiffs, who are appointed by an official act of government.

3. This Directive shall not apply to the field of taxation.

Article 3

Relationship with other provisions of Community law

1. If the provisions of this Directive conflict with a provision of another Community act governing specific aspects of access to or exercise of a service activity in specific sectors or for specific professions, the provision of the other Community act shall prevail and shall apply to those specific sectors or professions. These include:

(a) Directive 96/71/EC;

(b) Regulation (EEC) No 1408/71;

(c) 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 [1];

(d) Directive 2005/36/EC.

2. This Directive does not concern rules of private international law, in particular rules governing the law applicable to contractual and non contractual obligations, including those which guarantee that consumers benefit from the protection granted to them by the consumer protection rules laid down in the consumer legislation in force in their Member State.

[1] OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

3. Member States shall apply the provisions of this Directive in compliance with the rules of the Treaty on the right of establishment and the free movement of services.

Article 4

Definitions

For the purposes of this Directive, the following definitions shall apply:

1) 'service' means any self-employed economic activity, normally provided for remuneration, as referred to in Article 50 of the Treaty;

2) 'provider' means any natural person who is a national of a Member State, or any legal person as referred to in Article 48 of the Treaty and established in a Member State, who offers or provides a service;

3) 'recipient' means any natural person who is a national of a Member State or who benefits from rights conferred upon him by Community acts, or any legal person as referred to in Article 48 of the Treaty and established in a Member State, who, for professional or non-professional purposes, uses, or wishes to use, a service;

4) 'Member State of establishment' means the Member State in whose territory the provider of the service concerned is established;

5) 'establishment' means the actual pursuit of an economic activity, as referred to in Article 43 of the Treaty, by the provider for an indefinite period and through a stable infrastructure from where the business of providing services is actually carried out;

6) 'authorisation scheme' means any procedure under which a provider or recipient is in effect required to take steps in order to obtain from a competent authority a formal decision, or an implied decision, concerning access to a service activity or the exercise thereof;

7) 'requirement' means any obligation, prohibition, condition or limit provided for in the laws, regulations or administrative provisions of the Member States or in consequence of case-law, administrative practice, the rules of professional bodies, or the collective rules of professional associations or other professional organisations, adopted in the exercise of their legal autonomy; rules laid down in collective agreements negotiated by the social partners shall not as such be seen as requirements within the meaning of this Directive;

8) 'overriding reasons relating to the public interest' means reasons recognised as such in the case law of the Court of Justice, including the following grounds: public policy; public security; public safety; public health; preserving the financial equilibrium of the social security system; the protection of consumers, recipients of services and workers; fairness of trade transactions; combating fraud; the protection of the environment and the urban environment; the health of animals; intellectual property; the conservation of the national historic and artistic heritage; social policy objectives and cultural policy objectives;

9) 'competent authority' means any body or authority which has a supervisory or regulatory role in a Member State in relation to service activities, including, in particular, administrative authorities, including courts acting as such, professional bodies, and those professional associations or other professional organisations which, in the exercise of their legal autonomy, regulate in a collective manner access to service activities or the exercise thereof;

10) 'Member State where the service is provided' means the Member State where the service is supplied by a provider established in another Member State;

11) 'regulated profession' means a professional activity or a group of professional activities as referred to in Article 3(1)(a) of Directive 2005/36/EC;

12) 'commercial communication' means any form of communication designed to promote, directly or indirectly, the goods, services or image of an undertaking, organisation or person engaged in commercial, industrial or craft activity or practising a regulated profession. The following do not in themselves constitute commercial communications:

   (a) information enabling direct access to the activity of the undertaking, organisation or person, including in particular a domain name or an electronic-mailing address;

   (b) communications relating to the goods, services or image of the undertaking, organisation or person, compiled in an independent manner, particularly when provided for no financial consideration.

CHAPTER II

ADMINISTRATIVE SIMPLIFICATION

Article 5

Simplification of procedures

1. Member States shall examine the procedures and formalities applicable to access to a service activity and to the exercise thereof. Where procedures and formalities examined under this paragraph are not sufficiently simple, Member States shall simplify them.

2. The Commission may introduce harmonised forms at Community level, in accordance with the procedure referred to in Article 40(2). These forms shall be equivalent to certificates, attestations and any other documents required of a provider.

3. Where Member States require a provider or recipient to supply a certificate, attestation or any other document proving that a requirement has been satisfied, they shall accept any document from another Member State which serves an equivalent purpose or from which it is clear that the requirement in question has been satisfied. They may not require a document from another Member State to be produced in its original form, or as a certified copy or as a certified translation, save in the cases provided for in other Community instruments or where such a requirement is justified by an overriding reason relating to the public interest, including public order and security.

The first subparagraph shall not affect the right of Member States to require non-certified translations of documents in one of their official languages.

4. Paragraph 3 shall not apply to the documents referred to in Article 7(2) and 50 of Directive 2005/36/EC, in Articles 45(3), 46, 49 and 50 of Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts [1], in Article 3(2) of Directive 98/5/EC of the European Parliament and of the Council of 16 February 1998 to facilitate practice of the profession of lawyer on a permanent basis in a Member State other than that in which the qualification was obtained [2], in the First Council Directive 68/151/EEC of 9 March 1968 on coordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community [3] and in the Eleventh Council Directive 89/666/EECof 21 December 1989 concerning disclosure requirements in respect of branches opened in a Member State by certain types of company governed by the law of another State [4].

Article 6

Points of single contact

1. Member States shall ensure that it is possible for providers to complete the following procedures and formalities through points of single contact:

(a) all procedures and formalities needed for access to his service activities, in particular, all declarations, notifications or applications necessary for authorisation from the competent authorities, including applications for inclusion in a register, a roll or a database, or for registration with a professional body or association;

(b) any applications for authorisation needed to exercise his service activities.

2. The establishment of points of single contact shall be without prejudice to the allocation of functions and powers among the authorities within national systems.

Article 7

Right to information

1. Member States shall ensure that the following information is easily accessible to providers and recipients through the points of single contact:

(a) requirements applicable to providers established in their territory, in particular those requirements concerning the procedures and formalities to be completed in order to access and to exercise service activities;

(b) the contact details of the competent authorities enabling the latter to be contacted directly, including the details of those authorities responsible for matters concerning the exercise of service activities;

(c) the means of, and conditions for, accessing public registers and databases on providers and services;

(d) the means of redress which are generally available in the event of dispute between the competent authorities and the provider or the recipient, or between a provider and a recipient or between providers;

(e) the contact details of the associations or organisations, other than the competent authorities, from which providers or recipients may obtain practical assistance.

2. Member States shall ensure that it is possible for providers and recipients to receive, at their request, assistance from the competent authorities, consisting in information on the way in which the requirements referred to in point (a) of paragraph 1 are generally interpreted and applied. Where appropriate, such advice shall include a simple step-by-step guide. The information shall be provided in plain and intelligible language.

3. Member States shall ensure that the information and assistance referred to in paragraphs 1 and 2 are provided in a clear and unambiguous manner, that they are easily accessible at a distance and by electronic means and that they are kept up to date.

4. Member States shall ensure that the points of single contact and the competent authorities respond as quickly as possible to any request for information or assistance as referred to in paragraphs 1 and 2 and, in cases where the request is faulty or unfounded, inform the applicant accordingly without delay.

---

[1] OJ L 134, 30.4.2004, p. 114. Directive as last amended by Commission Regulation (EC) No 2083/2005 (OJ L 333, 20.12.2005, p. 28).

[2] OJ L 77, 14.3.1998, p. 36. Directive as amended by the 2003 Act of Accession.

[3] OJ L 65, 14.3.1968, p. 8. Directive as last amended by Directive 2003/58/EC of the European Parliament and of the Council (OJ L 221, 4.9.2003, p. 13).

[4] OJ L 395, 30.12.1989, p. 36.

5. Member States and the Commission shall take accompanying measures in order to encourage points of single contact to make the information provided for in this Article available in other Community languages. This does not interfere with Member States' legislation on the use of languages.

6. The obligation for competent authorities to assist providers and recipients does not require those authorities to provide legal advice in individual cases but concerns only general information on the way in which requirements are usually interpreted or applied.

Article 8

Procedures by electronic means

1. Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.

2. Paragraph 1 shall not apply to the inspection of premises on which the service is provided or of equipment used by the provider or to physical examination of the capability or of the personal integrity of the provider or of his responsible staff.

3. The Commission shall, in accordance with the procedure referred to in Article 40(2), adopt detailed rules for the implementation of paragraph 1 of this Article with a view to facilitating the interoperability of information systems and use of procedures by electronic means between Member States, taking into account common standards developed at Community level.

CHAPTER III

FREEDOM OF ESTABLISHMENT FOR PROVIDERS

SECTION 1

Authorisations

Article 9

Authorisation schemes

1. Member States shall not make access to a service activity or the exercise thereof subject to an authorisation scheme unless the following conditions are satisfied:

(a) the authorisation scheme does not discriminate against the provider in question;

(b) the need for an authorisation scheme is justified by an overriding reason relating to the public interest;

(c) the objective pursued cannot be attained by means of a less restrictive measure, in particular because an a posteriori inspection would take place too late to be genuinely effective.

2. In the report referred to in Article 39(1), Member States shall identify their authorisation schemes and give reasons showing their compatibility with paragraph 1 of this Article.

3. This section shall not apply to those aspects of authorisation schemes which are governed directly or indirectly by other Community instruments.

Article 10

Condiations for the granting of authorisation

1. Authorisation schemes shall be based on criteria which preclude the competent authorities from exercising their power of assessment in an arbitrary manner.

2. The criteria referred to in paragraph 1 shall be:

(a) non-discriminatory;

(b) justified by an overriding reason relating to the public interest;

(c) proportionate to that public interest objective;

(d) clear and unambiguous;

(e) objective;

(f) made public in advance;

(g) transparent and accessible.

3. The conditions for granting authorisation for a new establishment shall not duplicate requirements and controls which are equivalent or essentially comparable as regards their purpose to which the provider is already subject in another Member State or in the same Member State. The liaison points referred to in Article 28(2) and the provider shall assist the competent authority by providing any necessary information regarding those requirements.

4. The authorisation shall enable the provider to have access to the service activity, or to exercise that activity, throughout the national territory, including by means of setting up agencies, subsidiaries, branches or offices, except where an authorisation for each individual establishment or a limitation of the authorisation to a certain part of the territory is justified by an overriding reason relating to the public interest.

5. The authorisation shall be granted as soon as it is established, in the light of an appropriate examination, that the conditions for authorisation have been met.

6. Except in the case of the granting of an authorisation, any decision from the competent authorities, including refusal or withdrawal of an authorisation, shall be fully reasoned and shall be open to challenge before the courts or other instances of appeal.

7. This Article shall not call into question the allocation of the competences, at local or regional level, of the Member States' authorities granting authorisations.

Article 11

Duration of authorisation

1. An authorisation granted to a provider shall not be for a limited period, except where:

(a) the authorisation is being automatically renewed or is subject only to the continued fulfilment of requirements;

(b) the number of available authorisations is limited by an overriding reason relating to the public interest;

or

(c) a limited authorisation period can be justified by an overriding reason relating to the public interest.

2. Paragraph 1 shall not concern the maximum period before the end of which the provider must actually commence his activity after receiving authorisation.

3. Member States shall require a provider to inform the relevant point of single contact provided for in Article 6 of the following changes:

(a) the creation of subsidiaries whose activities fall within the scope of the authorisation scheme;

(b) changes in his situation which result in the conditions for authorisation no longer being met.

4. This Article shall be without prejudice to the Member States' ability to revoke authorisations, when the conditions for authorisation are no longer met.

Article 12

Selection from among several candidates

1. Where the number of authorisations available for a given activity is limited because of the scarcity of available natural resources or technical capacity, Member States shall apply a selection procedure to potential candidates which provides full guarantees of impartiality and transparency, including, in particular, adequate publicity about the launch, conduct and completion of the procedure.

2. In the cases referred to in paragraph 1, authorisation shall be granted for an appropriate limited period and may not be open to automatic renewal nor confer any other advantage on the provider whose authorisation has just expired or on any person having any particular links with that provider.

3. Subject to paragraph 1 and to Articles 9 and 10, Member States may take into account, in establishing the rules for the selection procedure, considerations of public health, social policy objectives, the health and safety of employees or self-employed persons, the protection of the environment, the preservation of cultural heritage and other overriding reasons relating to the public interest, in conformity with Community law.

Article 13

Authorisation procedures

1. Authorisation procedures and formalities shall be clear, made public in advance and be such as to provide the applicants with a guarantee that their application will be dealt with objectively and impartially.

2. Authorisation procedures and formalities shall not be dissuasive and shall not unduly complicate or delay the provision of the service. They shall be easily accessible and any charges which the applicants may incur from their application shall be reasonable and proportionate to the cost of the authorisation procedures in question and shall not exceed the cost of the procedures.

3. Authorisation procedures and formalities shall provide applicants with a guarantee that their application will be processed as quickly as possible and, in any event, within a reasonable period which is fixed and made public in advance. The period shall run only from the time when all documentation has been submitted. When justified by the complexity of the issue, the time period may be extended once, by the competent authority, for a limited time. The extension and its duration shall be duly motivated and shall be notified to the applicant before the original period has expired.

4. Failing a response within the time period set or extended in accordance with paragraph 3, authorisation shall be deemed to have been granted. Different arrangements may nevertheless be put in place, where justified by overriding reasons relating to the public interest, including a legitimate interest of third parties.

5. All applications for authorisation shall be acknowledged as quickly as possible. The acknowledgement must specify the following:

(a) the period referred to in paragraph 3;

(b) the available means of redress;

(c) where applicable, a statement that in the absence of a response within the period specified, the authorisation shall be deemed to have been granted.

6. In the case of an incomplete application, the applicant shall be informed as quickly as possible of the need to supply any additional documentation, as well as of any possible effects on the period referred to in paragraph 3.

7. When a request is rejected because it fails to comply with the required procedures or formalities, the applicant shall be informed of the rejection as quickly as possible.

SECTION 2

Requirements prohibited or subject to evaluation

Article 14

Prohibited requirements

Member States shall not make access to, or the exercise of, a service activity in their territory subject to compliance with any of the following:

1) discriminatory requirements based directly or indirectly on nationality or, in the case of companies, the location of the registered office, including in particular:

   (a) nationality requirements for the provider, his staff, persons holding the share capital or members of the provider's management or supervisory bodies;

   (b) a requirement that the provider, his staff, persons holding the share capital or members of the provider's management or supervisory bodies be resident within the territory;

2) a prohibition on having an establishment in more than one Member State or on being entered in the registers or enrolled with professional bodies or associations of more than one Member State;

3) restrictions on the freedom of a provider to choose between a principal or a secondary establishment, in particular an obligation on the provider to have its principal establishment in their territory, or restrictions on the freedom to choose between establishment in the form of an agency, branch or subsidiary;

4) conditions of reciprocity with the Member State in which the provider already has an establishment, save in the case of conditions of reciprocity provided for in Community instruments concerning energy;

5) the case-by-case application of an economic test making the granting of authorisation subject to proof of the existence of an economic need or market demand, an assessment of the potential or current economic effects of the activity or an assessment of the appropriateness of the activity in relation to the economic planning objectives set by the competent authority; this prohibition shall not concern planning requirements which do not pursue economic aims but serve overriding reasons relating to the public interest;

6) the direct or indirect involvement of competing operators, including within consultative bodies, in the granting of authorisations or in the adoption of other decisions of the competent authorities, with the exception of professional bodies and associations or other organisations acting as the competent authority; this prohibition shall not concern the consultation of organisations, such as chambers of commerce or social partners, on matters other than individual applications for authorisation, or a consultation of the public at large;

7) an obligation to provide or participate in a financial guarantee or to take out insurance from a provider or body established in their territory. This shall not affect the possibility for Member States to require insurance or financial guarantees as such, nor shall it affect requirements relating to the participation in a collective compensation fund, for instance for members of professional bodies or organisations;

8) an obligation to have been pre-registered, for a given period, in the registers held in their territory or to have previously exercised the activity for a given period in their territory.

Article 15

Requirements to be evaluated

1. Member States shall examine whether, under their legal system, any of the requirements listed in paragraph 2 are imposed and shall ensure that any such requirements are compatible with the conditions laid down in paragraph 3. Member States shall adapt their laws, regulations or administrative provisions so as to make them compatible with those conditions.

2. Member States shall examine whether their legal system makes access to a service activity or the exercise of it subject to compliance with any of the following non-discriminatory requirements:

(a) quantitative or territorial restrictions, in particular in the form of limits fixed according to population or of a minimum geographical distance between providers;

(b) an obligation on a provider to take a specific legal form;

(c) requirements which relate to the shareholding of a company;

(d) requirements, other than those concerning matters covered by Directive 2005/36/EC or provided for in other Community instruments, which reserve access to the service activity in question to particular providers by virtue of the specific nature of the activity;

(e) a ban on having more than one establishment in the territory of the same State;

(f) requirements fixing a minimum number of employees;

(g) fixed minimum and/or maximum tariffs with which the provider must comply;

(h) an obligation on the provider to supply other specific services jointly with his service.

3. Member States shall verify that the requirements referred to in paragraph 2 satisfy the following conditions:

(a) non-discrimination: requirements must be neither directly nor indirectly discriminatory according to nationality nor, with regard to companies, according to the location of the registered office;

(b) necessity: requirements must be justified by an overriding reason relating to the public interest;

(c) proportionality: requirements must be suitable for securing the attainment of the objective pursued; they must not go beyond what is necessary to attain that objective and it must not be possible to replace those requirements with other, less restrictive measures which attain the same result.

4. Paragraphs 1, 2 and 3 shall apply to legislation in the field of services of general economic interest only insofar as the application of these paragraphs does not obstruct the performance, in law or in fact, of the particular task assigned to them.

5. In the mutual evaluation report provided for in Article 39(1), Member States shall specify the following:

(a) the requirements that they intend to maintain and the reasons why they consider that those requirements comply with the conditions set out in paragraph 3;

(b) the requirements which have been abolished or made less stringent.

6. From 28 December 2006 Member States shall not introduce any new requirement of a kind listed in paragraph 2, unless that requirement satisfies the conditions laid down in paragraph 3.

7. Member States shall notify the Commission of any new laws, regulations or administrative provisions which set requirements as referred to in paragraph 6, together with the reasons for those requirements. The Commission shall communicate the provisions concerned to the other Member States. Such notification shall not prevent Member States from adopting the provisions in question.

Within a period of 3 months from the date of receipt of the notification, the Commission shall examine the compatibility of any new requirements with Community law and, where appropriate, shall adopt a decision requesting the Member State in question to refrain from adopting them or to abolish them.

The notification of a draft national law in accordance with Directive 98/34/EC shall fulfil the obligation of notification provided for in this Directive.

CHAPTER IV

FREE MOVEMENT OF SERVICES

SECTION 1

Freedom to provide services and related derogations

Article 16

Freedom to provide services

1. Member States shall respect the right of providers to provide services in a Member State other than that in which they are established.

The Member State in which the service is provided shall ensure free access to and free exercise of a service activity within its territory.

Member States shall not make access to or exercise of a service activity in their territory subject to compliance with any requirements which do not respect the following principles:

(a) non-discrimination: the requirement may be neither directly nor indirectly discriminatory with regard to nationality or, in the case of legal persons, with regard to the Member State in which they are established;

(b) necessity: the requirement must be justified for reasons of public policy, public security, public health or the protection of the environment;

(c) proportionality: the requirement must be suitable for attaining the objective pursued, and must not go beyond what is necessary to attain that objective.

2. Member States may not restrict the freedom to provide services in the case of a provider established in another Member State by imposing any of the following requirements:

(a) an obligation on the provider to have an establishment in their territory;

(b) an obligation on the provider to obtain an authorisation from their competent authorities including entry in a register or registration with a professional body or association in their territory, except where provided for in this Directive or other instruments of Community law;

(c) a ban on the provider setting up a certain form or type of infrastructure in their territory, including an office or chambers, which the provider needs in order to supply the services in question;

(d) the application of specific contractual arrangements between the provider and the recipient which prevent or restrict service provision by the self-employed;

(e) an obligation on the provider to possess an identity document issued by its competent authorities specific to the exercise of a service activity;

(f) requirements, except for those necessary for health and safety at work, which affect the use of equipment and material which are an integral part of the service provided;

(g) restrictions on the freedom to provide the services referred to in Article 19.

3. The Member State to which the provider moves shall not be prevented from imposing requirements with regard to the provision of a service activity, where they are justified for reasons of public policy, public security, public health or the protection of the environment and in accordance with paragraph 1. Nor shall that Member State be prevented from applying, in accordance with Community law, its rules on employment conditions, including those laid down in collective agreements.

4. By 28 December 2011 the Commission shall, after consultation of the Member States and the social partners at Community level, submit to the European Parliament and the Council a report on the application of this Article, in which it shall consider the need to propose harmonisation measures regarding service activities covered by this Directive.

Article 17

Additional derogations from the freedom to provide services

Article 16 shall not apply to:

1) services of general economic interest which are provided in another Member State, inter alia:

   (a) in the postal sector, 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 ([1]);

   (b) in the electricity sector, services covered by Directive 2003/54/EC ([2]) of the European Parliament and of the Council of 26 June 2003 concerning common rules for the internal market in electricity;

   (c) in the gas sector, services covered by Directive 2003/55/EC of the European Parliament and of the Council of 26 June 2003 concerning common rules for the internal market in natural gas ([3]);

   (d) water distribution and supply services and waste water services;

   (e) treatment of waste;

2) matters covered by Directive 96/71/EC;

3) matters covered by 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]);

4) matters covered by Council Directive 77/249/EEC of 22 March 1977to facilitate the effective exercise by lawyers of freedom to provide services ([5]);

5) the activity of judicial recovery of debts;

([1]) OJ L 15, 21.1.1998, p. 14. Directive as last amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

([2]) OJ L 176, 15.7.2003, p. 37. Directive as last amended by Commission Decision 2006/653/EC (OJ L 270, 29.9.2006, p. 72).

([3]) OJ L 176, 15.7.2003, p. 57.

([4]) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003.

([5]) OJ L 78, 26.3.1977, p. 17. Directive as last amended by the 2003 Act of Accession.

6) matters covered by Title II of Directive 2005/36/EC, as well as requirements in the Member State where the service is provided which reserve an activity to a particular profession;

7) matters covered by Regulation (EEC) No 1408/71;

8) as regards administrative formalities concerning the free movement of persons and their residence, matters covered by the provisions of Directive 2004/38/EC that lay down administrative formalities of the competent authorities of the Member Statewhere the service is provided with which beneficiaries must comply;

9) as regards third country nationals who move to another Member State in the context of the provision of a service, the possibility for Member States to require visa or residence permits for third country nationals who are not covered by the mutual recognition regime provided for in Article 21 of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders [1] or the possibility to oblige third country nationals to report to the competent authorities of the Member State in which the service is provided on or after their entry;

10) as regards the shipment of waste, matters covered by Council Regulation (EEC) No 259/93 of 1 February 1993 on the supervision and control of shipments of waste within, into and out of the European Community [2];

11) copyright, neighbouring rights and rights covered by Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products [3] and by Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [4], as well as industrial property rights;

12) acts requiring by law the involvement of a notary;

13) matters covered by Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audit of annual accounts and consolidated accounts [5];

14) the registration of vehicles leased in another Member State;

15) provisions regarding contractual and non-contractual obligations, including the form of contracts, determined pursuant to the rules of private international law.

Article 18

Case-by-case derogations

1. By way of derogation from Article 16, and in exceptional circumstances only, a Member State may, in respect of a provider established in another Member State, take measures relating to the safety of services.

2. The measures provided for in paragraph 1 may be taken only if the mutual assistance procedure laid down in Article 35 is complied with and the following conditions are fulfilled:

(a) the national provisions in accordance with which the measure is taken have not been subject to Community harmonisation in the field of the safety of services;

(b) the measures provide for a higher level of protection of the recipient than would be the case in a measure taken by the Member State of establishment in accordance with its national provisions;

(c) the Member State of establishment has not taken any measures or has taken measures which are insufficient as compared with those referred to in Article 35(2);

(d) the measures are proportionate.

3. Paragraphs 1 and 2 shall be without prejudice to provisions, laid down in Community instruments, which guarantee the freedom to provide services or which allow derogations therefrom.

SECTION 2

Rights of recipients of services

Article 19

Prohibited restrictions

Member States may not impose on a recipient requirements which restrict the use of a service supplied by a provider established in another Member State, in particular the following requirements:

(a) an obligation to obtain authorisation from or to make a declaration to their competent authorities;

---

[1] OJ L 239, 22.9.2000, p. 19. Convention as last amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).

[2] OJ L 30, 6.2.1993, p. 1. Regulation as last amended by Commission Regulation (EC) No 2557/2001 (OJ L 349, 31.12.2001, p. 1).

[3] OJ L 24, 27.1.1987, p. 36.

[4] OJ L 77, 27.3.1996, p. 20.

[5] OJ L 157, 9.6.2006, p. 87.

(b) discriminatory limits on the grant of financial assistance by reason of the fact that the provider is established in another Member State or by reason of the location of the place at which the service is provided.

Article 20

Non-discrimination

1. Member States shall ensure that the recipient is not made subject to discriminatory requirements based on his nationality or place of residence.

2. Member States shall ensure that the general conditions of access to a service, which are made available to the public at large by the provider, do not contain discriminatory provisions relating to the nationality or place of residence of the recipient, but without precluding the possibility of providing for differences in the conditions of access where those differences are directly justified by objective criteria.

Article 21

Assistance for recipients

1. Member States shall ensure that recipients can obtain, in their Member State of residence, the following information:

(a) general information on the requirements applicable in other Member States relating to access to, and exercise of, service activities, in particular those relating to consumer protection;

(b) general information on the means of redress available in the case of a dispute between a provider and a recipient;

(c) the contact details of associations or organisations, including the centres of the European Consumer Centres Network, from which providers or recipients may obtain practical assistance.

Where appropriate, advice from the competent authorities shall include a simple step-by-step guide. Information and assistance shall be provided in a clear and unambiguous manner, shall be easily accessible at a distance, including by electronic means, and shall be kept up to date.

2. Member States may confer responsibility for the task referred to in paragraph 1 on points of single contact or on any other body, such as the centres of the European Consumer Centres Network, consumer associations or Euro Info Centres.

Member States shall communicate to the Commission the names and contact details of the designated bodies. The Commission shall transmit them to all Member States.

3. In fulfilment of the requirements set out in paragraphs 1 and 2, the body approached by the recipient shall, if necessary, contact the relevant body for the Member State concerned. The latter shall send the information requested as soon as possible to the requesting body which shall forward the information to the recipient. Member States shall ensure that those bodies give each other mutual assistance and shall put in place all possible measures for effective cooperation. Together with the Commission, Member States shall put in place practical arrangements necessary for the implementation of paragraph 1.

4. The Commission shall, in accordance with the procedure referred to in Article 40(2), adopt measures for the implementation of paragraphs 1, 2 and 3 of this Article, specifying the technical mechanisms for the exchange of information between the bodies of the various Member States and, in particular, the interoperability of information systems, taking into account common standards.

CHAPTER V

QUALITY OF SERVICES

Article 22

Information on providers and their services

1. Member States shall ensure that providers make the following information available to the recipient:

(a) the name of the provider, his legal status and form, the geographic address at which he is established and details enabling him to be contacted rapidly and communicated with directly and, as the case may be, by electronic means;

(b) where the provider is registered in a trade or other similar public register, the name of that register and the provider's registration number, or equivalent means of identification in that register;

(c) where the activity is subject to an authorisation scheme, the particulars of the relevant competent authority or the single point of contact;

(d) where the provider exercises an activity which is subject to VAT, the identification number referred to in Article 22(1) of 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 [1];

[1] OJ L 145, 13.6.1977, p. 1. Directive as last amended by Directive 2006/18/EC (OJ L 51, 22.2.2006, p. 12).

(e) in the case of the regulated professions, any professional body or similar institution with which the provider is registered, the professional title and the Member State in which that title has been granted;

(f) the general conditions and clauses, if any, used by the provider;

(g) the existence of contractual clauses, if any, used by the provider concerning the law applicable to the contract and/or the competent courts;

(h) the existence of an after-sales guarantee, if any, not imposed by law;

(i) the price of the service, where a price is pre-determined by the provider for a given type of service;

(j) the main features of the service, if not already apparent from the context;

(k) the insurance or guarantees referred to in Article 23(1), and in particular the contact details of the insurer or guarantor and the territorial coverage.

2. Member States shall ensure that the information referred to in paragraph 1, according to the provider's preference:

(a) is supplied by the provider on his own initiative;

(b) is easily accessible to the recipient at the place where the service is provided or the contract concluded;

(c) can be easily accessed by the recipient electronically by means of an address supplied by the provider;

(d) appears in any information documents supplied to the recipient by the provider which set out a detailed description of the service he provides.

3. Member States shall ensure that, at the recipient's request, providers supply the following additional information:

(a) where the price is not pre-determined by the provider for a given type of service, the price of the service or, if an exact price cannot be given, the method for calculating the price so that it can be checked by the recipient, or a sufficiently detailed estimate;

(b) as regards the regulated professions, a reference to the professional rules applicable in the Member State of establishment and how to access them;

(c) information on their multidisciplinary activities and partnerships which are directly linked to the service in question and on the measures taken to avoid conflicts of interest. That information shall be included in any information document in which providers give a detailed description of their services;

(d) any codes of conduct to which the provider is subject and the address at which these codes may be consulted by electronic means, specifying the language version available;

(e) where a provider is subject to a code of conduct, or member of a trade association or professional body which provides for recourse to a non-judicial means of dispute settlement, information in this respect. The provider shall specify how to access detailed information on the characteristics of, and conditions for, the use of non-judicial means of dispute settlement.

4. Member States shall ensure that the information which a provider must supply in accordance with this Chapter is made available or communicated in a clear and unambiguous manner, and in good time before conclusion of the contract or, where there is no written contract, before the service is provided.

5. The information requirements laid down in this Chapter are in addition to requirements already provided for in Community law and do not prevent Member States from imposing additional information requirements applicable to providers established in their territory.

6. The Commission may, in accordance with the procedure referred to in Article 40(2), specify the content of the information provided for in paragraphs 1 and 3 of this Article according to the specific nature of certain activities and may specify the practical means of implementing paragraph 2 of this Article.

Article 23

Professional liability insurance and guarantees

1. Member States may ensure that providers whose services present a direct and particular risk to the health or safety of the recipient or a third person, or to the financial security of the recipient, subscribe to professional liability insurance appropriate to the nature and extent of the risk, or provide a guarantee or similar arrangement which is equivalent or essentially comparable as regards its purpose.

2. When a provider establishes himself in their territory, Member States may not require professional liability insurance or a guarantee from the provider where he is already covered by a guarantee which is equivalent, or essentially comparable as regards its purpose and the cover it provides in terms of the insured risk, the insured sum or a ceiling for the guarantee and possible exclusions from the cover, in another Member State in which the provider is already established. Where equivalence is only partial, Member States may require a supplementary guarantee to cover those aspects not already covered.

When a Member State requires a provider established in its territory to subscribe to professional liability insurance or to provide another guarantee, that Member State shall accept as sufficient evidence attestations of such insurance cover issued by credit institutions and insurers established in other Member States.

3. Paragraphs 1 and 2 shall not affect professional insurance or guarantee arrangements provided for in other Community instruments.

4. For the implementation of paragraph 1, the Commission may, in accordance with the regulatory procedure referred to in Article 40(2), establish a list of services which exhibit the characteristics referred to in paragraph 1 of this Article. The Commission may also, in accordance with the procedure referred to in Article 40(3), adopt measures designed to amend non-essential elements of this Directive by supplementing it by establishing common criteria for defining, for the purposes of the insurance or guarantees referred to in paragraph 1 of this Article, what is appropriate to the nature and extent of the risk.

5. For the purpose of this Article

— 'direct and particular risk' means a risk arising directly from the provision of the service,

— 'health and safety' means, in relation to a recipient or a third person, the prevention of death or serious personal injury,

— 'financial security' means, in relation to a recipient, the prevention of substantial losses of money or of value of property,

— 'professional liability insurance' means insurance taken out by a provider in respect of potential liabilities to recipients and, where applicable, third parties arising out of the provision of the service.

Article 24

Commercial communications by the regulated professions

1. Member States shall remove all total prohibitions on commercial communications by the regulated professions.

2. Member States shall ensure that commercial communications by the regulated professions comply with professional rules, in conformity with Community law, which relate, in particular, to the independence, dignity and integrity of the profession, as well as to professional secrecy, in a manner consistent with the specific nature of each profession. Professional rules on commercial communications shall be non-discriminatory, justified by an overriding reason relating to the public interest and proportionate.

Article 25

Multidisciplinary activities

1. Member States shall ensure that providers are not made subject to requirements which oblige them to exercise a given specific activity exclusively or which restrict the exercise jointly or in partnership of different activities.

However, the following providers may be made subject to such requirements:

(a) the regulated professions, in so far as is justified in order to guarantee compliance with the rules governing professional ethics and conduct, which vary according to the specific nature of each profession, and is necessary in order to ensure their independence and impartiality;

(b) providers of certification, accreditation, technical monitoring, test or trial services, in so far as is justified in order to ensure their independence and impartiality.

2. Where multidisciplinary activities between providers referred to in points (a) and (b) of paragraph 1 are authorised, Member States shall ensure the following:

(a) that conflicts of interest and incompatibilities between certain activities are prevented;

(b) that the independence and impartiality required for certain activities is secured;

(c) that the rules governing professional ethics and conduct for different activities are compatible with one another, especially as regards matters of professional secrecy.

3. In the report referred to in Article 39(1), Member States shall indicate which providers are subject to the requirements laid down in paragraph 1 of this Article, the content of those requirements and the reasons for which they consider them to be justified.

Article 26

Policy on quality of services

1. Member States shall, in cooperation with the Commission, take accompanying measures to encourage providers to take action on a voluntary basis in order to ensure the quality of service provision, in particular through use of one of the following methods:

(a) certification or assessment of their activities by independent or accredited bodies;

(b) drawing up their own quality charter or participation in quality charters or labels drawn up by professional bodies at Community level.

2. Member States shall ensure that information on the significance of certain labels and the criteria for applying labels and other quality marks relating to services can be easily accessed by providers and recipients.

3. Member States shall, in cooperation with the Commission, take accompanying measures to encourage professional bodies, as well as chambers of commerce and craft associationsand consumer associations, in their territory to cooperate at Community level in order to promote the quality of service provision, especially by making it easier to assess the competence of a provider.

4. Member States shall, in cooperation with the Commission, take accompanying measures to encourage the development of independent assessments, notably by consumer associations, in relation to the quality and defects of service provision, and, in particular, the development at Community level of comparative trials or testing and the communication of the results.

5. Member States, in cooperation with the Commission, shall encourage the development of voluntary European standards with the aim of facilitating compatibility between services supplied by providers in different Member States, information to the recipient and the quality of service provision.

Article 27

Settlement of disputes

1. Member States shall take the general measures necessary to ensure that providers supply contact details, in particular a postal address, fax number or e-mail addressand telephone number to which all recipients, including those resident in another Member State, can send a complaint or a request for information about the service provided. Providers shall supply their legal address if this is not their usual address for correspondence.

Member States shall take the general measures necessary to ensure that providers respond to the complaints referred to in the first subparagraph in the shortest possible time and make their best efforts to find a satisfactory solution.

2. Member States shall take the general measures necessary to ensure that providers are obliged to demonstrate compliance with the obligations laid down in this Directive as to the provision of information and to demonstrate that the information is accurate.

3. Where a financial guarantee is required for compliance with a judicial decision, Member States shall recognise equivalent guarantees lodged with a credit institution or insurer established in another Member State. Such credit institutions must be authorised in a Member State in accordance with Directive 2006/48/EC and such insurers in accordance, as appropriate, with 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 [1] and Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance [2].

4. Member States shall take the general measures necessary to ensure that providers who are subject to a code of conduct, or are members of a trade association or professional body, which provides for recourse to a non-judicial means of dispute settlement inform the recipient thereof and mention that fact in any document which presents their services in detail, specifying how to access detailed information on the characteristics of, and conditions for, the use of such a mechanism.

CHAPTER VI

ADMINISTRATIVE COOPERATION

Article 28

Mutual assistance – general obligations

1. Member States shall give each other mutual assistance, and shall put in place measures for effective cooperation with one another, in order to ensure the supervision of providers and the services they provide.

2. For the purposes of this Chapter, Member States shall designate one or more liaison points, the contact details of which shall be communicated to the other Member States and the Commission. The Commission shall publish and regularly update the list of liaison points.

---

[1] OJ L 228, 16.8.1973, p. 3. Directive as last amended by Directive 2005/68/EC of the European Parliament and of the Council (OJ L 323, 9.12.2005, p. 1).

[2] OJ L 345, 19.12.2002, p. 1. Directive as last amended by Directive 2005/68/EC.

3. Information requests and requests to carry out any checks, inspections and investigations under this Chapter shall be duly motivated, in particular by specifying the reason for the request. Information exchanged shall be used only in respect of the matter for which it was requested.

4. In the event of receiving a request for assistance from competent authorities in another Member State, Member States shall ensure that providers established in their territory supply their competent authorities with all the information necessary for supervising their activities in compliance with their national laws.

5. In the event of difficulty in meeting a request for information or in carrying out checks, inspections or investigations, the Member State in question shall rapidly inform the requesting Member State with a view to finding a solution.

6. Member States shall supply the information requested by other Member States or the Commission by electronic means and within the shortest possible period of time.

7. Member States shall ensure that registers in which providers have been entered, and which may be consulted by the competent authorities in their territory, may also be consulted, in accordance with the same conditions, by the equivalent competent authorities of the other Member States.

8. Member States shall communicate to the Commission information on cases where other Member States do not fulfil their obligation of mutual assistance. Where necessary, the Commission shall take appropriate steps, including proceedings provided for in Article 226 of the Treaty, in order to ensure that the Member States concerned comply with their obligation of mutual assistance. The Commission shall periodically inform Member States about the functioning of the mutual assistance provisions.

Article 29

Mutual assistance – general obligations for the Member State of establishment

1. With respect to providers providing services in another Member State, the Member State of establishment shall supply information on providers established in its territory when requested to do so by another Member State and, in particular, confirmation that a provider is established in its territory and, to its knowledge, is not exercising his activities in an unlawful manner.

2. The Member State of establishment shall undertake the checks, inspections and investigations requested by another Member State and shall inform the latter of the results and, as the case may be, of the measures taken. In so doing, the competent authorities shall act to the extent permitted by the powers vested in them in their Member State. The competent authorities can decide on the most appropriate measures to be taken in each individual case in order to meet the request by another Member State.

3. Upon gaining actual knowledge of any conduct or specific acts by a provider established in its territory which provides services in other Member States, that, to its knowledge, could cause serious damage to the health or safety of persons or to the environment, the Member State of establishment shall inform all other Member States and the Commission within the shortest possible period of time.

Article 30

Supervision by the Member State of establishment in the event of the temporary movement of a provider to another Member State

1. With respect to cases not covered by Article 31(1), the Member State of establishment shall ensure that compliance with its requirementsis supervised in conformity with the powers of supervision provided for in its national law, in particular through supervisory measures at the place of establishment of the provider.

2. The Member State of establishment shall not refrain from taking supervisory or enforcement measures in its territory on the grounds that the service has been provided or caused damage in another Member State.

3. The obligation laid down in paragraph 1 shall not entail a duty on the part of the Member State of establishment to carry out factual checks and controls in the territory of the Member State where the service is provided. Such checks and controls shall be carried out by the authorities of the Member State where the provider is temporarily operating at the request of the authorities of the Member State of establishment, in accordance with Article 31.

Article 31

Supervision by the Member State where the service is provided in the event of the temporary movement of the provider

1. With respect to national requirements which may be imposed pursuant to Articles 16 or 17, the Member State where the service is provided is responsible for the supervision of the activity of the provider in its territory. In conformity with Community law, the Member State where the service is provided:

(a) shall take all measures necessary to ensure the provider complies with those requirements as regards the access to and the exercise of the activity;

(b) shall carry out the checks, inspections and investigations necessary to supervise the service provided.

2. With respect to requirements other than those referred to in paragraph 1, where a provider moves temporarily to another Member State in order to provide a service without being established there, the competent authorities of that Member State shall participate in the supervision of the provider in accordance with paragraphs 3 and 4.

3. At the request of the Member State of establishment, the competent authorities of the Member State where the service is provided shall carry out any checks, inspections and investigations necessary for ensuring the effective supervision by the Member State of establishment. In so doing, the competent authorities shall act to the extent permitted by the powers vested in them in their Member State. The competent authorities may decide on the most appropriate measures to be taken in each individual case in order to meet the request by the Member State of establishment.

4. On their own initiative, the competent authorities of the Member State where the service is provided may conduct checks, inspections and investigations on the spot, provided that those checks, inspections or investigations are not discriminatory, are not motivated by the fact that the provider is established in another Member State and are proportionate.

Article 32

Alert mechanism

1. Where a Member State becomes aware of serious specific acts or circumstances relating to a service activity that could cause serious damage to the health or safety of persons or to the environment in its territory or in the territory of other Member States, that Member State shall inform the Member State of establishment, the other Member States concerned and the Commission within the shortest possible period of time.

2. The Commission shall promote and take part in the operation of a European network of Member States' authorities in order to implement paragraph 1.

3. The Commission shall adopt and regularly update, in accordance with the procedure referred to in Article 40(2), detailed rules concerning the management of the network referred to in paragraph 2 of this Article.

Article 33

Information on the good repute of providers

1. Member States shall, at the request of a competent authority in another Member State, supply information, in conformity with their national law, on disciplinary or administrative actions or criminal sanctions and decisions concerning insolvency or bankruptcy involving fraud taken by their competent authorities in respect of the provider which are directly relevant to the provider's competence or professional reliability. The Member State which supplies the information shall inform the provider thereof. A request made pursuant to the first subparagraph must be duly substantiated, in particular as regards the reasons for the request for information.

2. Sanctions and actions referred to in paragraph 1 shall only be communicated if a final decision has been taken. With regard to other enforceable decisions referred to in paragraph 1, the Member State which supplies the information shall specify whether a particular decision is final or whether an appeal has been lodged in respect of it, in which case the Member State in question should provide an indication of the date when the decision on appeal is expected.

Moreover, that Member State shall specify the provisions of national law pursuant to which the provider was found guilty or penalised.

3. Implementation of paragraphs 1and 2 must comply with rules on the provision of personal dataand with rights guaranteed to persons found guilty or penalised in the Member States concerned, including by professional bodies. Any information in question which is public shall be accessible to consumers.

Article 34

Accompanying measures

1. The Commission, in cooperation with Member States, shall establish an electronic system for the exchange of information between Member States, taking into account existing information systems.

2. Member States shall, with the assistance of the Commission, take accompanying measures to facilitate the exchange of officials in charge of the implementation of mutual assistance and training of such officials, including language and computer training.

3. The Commission shall assess the need to establish a multiannual programme in order to organise relevant exchanges of officials and training.

Article 35

Mutual assistance in the event of case-by-case derogations

1. Where a Member State intends to take a measure pursuant to Article 18, the procedure laid down in paragraphs 2 to 6 of this Article shall apply without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation.

2. The Member State referred to in paragraph 1 shall ask the Member State of establishment to take measures with regard to the provider, supplying all relevant information on the service in question and the circumstances of the case.

The Member State of establishment shall check, within the shortest possible period of time, whether the provider is operating lawfully and verify the facts underlying the request. It shall inform the requesting Member State within the shortest possible period of time of the measures taken or envisaged or, as the case may be, the reasons why it has not taken any measures.

3. Following communication by the Member State of establishment as provided for in the second subparagraph of paragraph 2, the requesting Member State shall notify the Commission and the Member State of establishment of its intention to take measures, stating the following:

(a) the reasons why it believes the measures taken or envisaged by the Member State of establishment are inadequate;

(b) the reasons why it believes the measures it intends to take fulfil the conditions laid down in Article 18.

4. The measures may not be taken until fifteen working days after the date of notification provided for in paragraph 3.

5. Without prejudice to the possibility for the requesting Member State to take the measures in question upon expiry of the period specified in paragraph 4, the Commission shall, within the shortest possible period of time, examine the compatibility with Community law of the measures notified.

Where the Commission concludes that the measure is incompatible with Community law, it shall adopt a decision asking the Member State concerned to refrain from taking the proposed measures or to put an end to the measures in question as a matter of urgency.

6. In the case of urgency, a Member State which intends to take a measure may derogate from paragraphs 2, 3 and 4. In such cases, the measures shall be notified within the shortest possible period of time to the Commission and the Member State of establishment, stating the reasons for which the Member State considers that there is urgency.

Article 36

Implementing measures

In accordance with the procedure referred to in Article 40(3), the Commission shall adopt the implementing measures designed to amend non-essential elements of this Chapter by supplementing it by specifying the time-limits provided for in Articles 28 and 35. The Commission shall also adopt, in accordance with the procedure referred to in Article 40(2), the practical arrangements for the exchange of information by electronic means between Member States, and in particular the interoperability provisions for information systems.

CHAPTER VII

CONVERGENCE PROGRAMME

Article 37

Codes of conduct at Community level

1. Member States shall, in cooperation with the Commission, take accompanying measures to encourage the drawing up at Community level, particularly by professional bodies, organisations and associations, of codes of conduct aimed at facilitating the provision of services or the establishment of a provider in another Member State, in conformity with Community law.

2. Member States shall ensure that the codes of conduct referred to in paragraph 1 are accessible at a distance, by electronic means.

Article 38

Additional harmonisation

The Commission shall assess, by 28 December 2010 the possibility of presenting proposals for harmonisation instruments on the following subjects:

(a) access to the activity of judicial recovery of debts;

(b) private security services and transport of cash and valuables.

Article 39

Mutual evaluation

1. By 28 December 2009 at the latest, Member States shall present a report to the Commission, containing the information specified in the following provisions:

(a) Article 9(2), on authorisation schemes;

(b) Article 15(5), on requirements to be evaluated;

(c) Article 25(3), on multidisciplinary activities.

2. The Commission shall forward the reports provided for in paragraph 1 to the Member States, which shall submit their observations on each of the reports within six months of receipt. Within the same period, the Commission shall consult interested parties on those reports.

3. The Commission shall present the reports and the Member States' observations to the Committee referred to in Article 40(1), which may make observations.

4. In the light of the observations provided for in paragraphs 2 and 3, the Commission shall, by 28 December 2010 at the latest, present a summary report to the European Parliament and to the Council, accompanied where appropriate by proposals for additional initiatives.

5. By 28 December 2009 at the latest, Member States shall present a report to the Commission on the national requirements whose application could fall under the third subparagraph of Article 16(1) and the first sentence of Article 16(3), providing reasons why they consider that the application of those requirements fulfil the criteria referred to in the third subparagraph of Article 16(1) and the first sentence of Article 16(3).

Thereafter, Member States shall transmit to the Commission any changes in their requirements, including new requirements, as referred to above, together with the reasons for them.

The Commission shall communicate the transmitted requirements to other Member States. Such transmission shall not prevent the adoption by Member States of the provisions in question. The Commission shall on an annual basis thereafter provide analyses and orientations on the application of these provisions in the context of this Directive.

Article 40

Committee procedure

1. The Commission shall be assisted by a Committee.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof. The period laid down in Article 5(6) 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.

Article 41

Review clause

The Commission, by 28 December 2011 and every three years thereafter, shall present to the European Parliament and to the Council a comprehensive report on the application of this Directive. This report shall, in accordance with Article 16(4), address in particular the application of Article 16. It shall also consider the need for additional measures for matters excluded from the scope of application of this Directive. It shall be accompanied, where appropriate, by proposals for amendment of this Directive with a view to completing the Internal Market for services.

Article 42

Amendment of Directive 98/27/EC

In the Annex to Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests [1], the following point shall be added:

'13. Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36)'.

Article 43

Protection of personal data

The implementation and application of this Directive and, in particular, the provisions on supervision shall respect the rules on the protection of personal data as provided for in Directives 95/46/EC and 2002/58/EC.

CHAPTER VIII

FINAL PROVISIONS

Article 44

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 28 December 2009.

They shall forthwith communicate to the Commission the text of those measures.

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 Member States.

[1] OJ L 166, 11.6.1998, p. 51. Directive as last amended by Directive 2005/29/EC.

2. 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 45

Entry into force

This Directive shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Article 46

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 12 December 2006.

For the European Parliament	*For the Council*
The President	*The President*
J. BORRELL FONTELLES	M. PEKKARINEN

DIRECTIVES

DIRECTIVE 2011/83/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 October 2011

on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

(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:

(1) Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises [4] and 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 [5] lay down a number of contractual rights for consumers.

(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 significant growth of domestic distance sales over 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

[1] OJ C 317, 23.12.2009, p. 54.
[2] OJ C 200, 25.8.2009, p. 76.
[3] Position of the European Parliament of 23 June 2011 (not yet published in the Official Journal) and decision of the Council of 10 October 2011.
[4] OJ L 372, 31.12.1985, p. 31.
[5] OJ L 144, 4.6.1997, p. 19.

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 employment, 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 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [1].

(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 complete the information requirements of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2] and 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') [3]. Member States should retain the possibility to impose additional information requirements applicable to service providers established in their territory.

(13) Member States should remain competent, in accordance with Union law, to apply the provisions of this Directive to areas not falling within its scope. 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 because they are not concluded under an organised distance sales or service-provision scheme. Moreover, Member States may also maintain or introduce national provisions on issues not specifically addressed in this Directive, such as additional rules concerning sales contracts, including in relation to the delivery of goods, or requirements for the provision of information during the existence of a contract.

(14) This Directive should not affect national law in the area of contract law for contract law aspects that are not regulated by this Directive. Therefore, this Directive should be without prejudice to national law regulating for instance the conclusion or the validity of a contract (for instance in the case of lack of consent). Similarly, this Directive should not affect national law in relation to the general contractual legal remedies, the rules on public economic order, for instance rules on excessive or extortionate prices, and the rules on unethical legal transactions.

[1] OJ L 177, 4.7.2008, p. 6.

[2] OJ L 376, 27.12.2006, p. 36.

[3] OJ L 178, 17.7.2000, p. 1.

(15) This Directive should not harmonise language requirements applicable to consumer contracts. Therefore, Member States may maintain or introduce in their national law language requirements regarding contractual information and contractual terms.

(16) This Directive should not affect national laws on legal representation such as the rules relating to the person who is acting in the name of the trader or on his behalf (such as an agent or a trustee). Member States should remain competent in this area. This Directive should apply to all traders, whether public or private.

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

(18) This Directive does not affect the freedom of Member States to define, in conformity with Union law, what they consider to be services of general economic interest, how those services should be organised and financed, in compliance with State aid rules, and which specific obligations they should be subject to.

(19) Digital content means data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means. Contracts for the supply of digital content should fall within the scope of this Directive. If digital content is supplied on a tangible medium, such as a CD or a DVD, it should be considered as goods within the meaning of this Directive. Similarly 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, or of district heating, contracts for digital content which is not supplied on a tangible medium should be classified, for the purpose of this Directive, neither as sales contracts nor as service contracts. For such contracts, the consumer should have a right of withdrawal unless he has consented to the beginning of the performance of the contract during the withdrawal period and has acknowledged that he will consequently lose the right to withdraw from the contract. In addition to the general information requirements, the trader should inform the consumer about the functionality and the relevant interoperability of digital content. The notion of functionality should refer to the ways in which digital content can be used, 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 is meant to describe the information regarding the standard hardware and software environment 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 fax) up to 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 consumer through a means of distance communications to request the provision of a service from a professional, such as in the case of a consumer phoning to request an appointment with a hairdresser. The notion of an organised distance sales or service-provision scheme should include those schemes offered by a third party other than the trader but used by the trader, such as an online platform. It should not, however, cover cases where websites merely offer information on the trader, his goods and/or services and his contact details.

(21) An off-premises contract should be defined as a contract concluded with the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader, for example at the consumer's home or workplace. In an off-premises context, the consumer may be under potential psychological pressure or may be confronted with an element of surprise, irrespective of whether or not the consumer has solicited the trader's visit. The definition of an off-premises contract should also include situations where the consumer is personally and individually addressed in an off-premises context but the contract is concluded immediately afterwards on the business premises of the trader or through a means of distance communication. The definition of an off-premises contract should not cover situations in which the

trader first comes to the consumer's home strictly with a view to taking measurements or giving an estimate without any commitment of the consumer and where the contract is then concluded only at a later point in time on the business premises of the trader or via means of distance communication on the basis of the trader's estimate. In those cases, the contract is not to be considered as having been concluded immediately after the trader has addressed the consumer if the consumer has had time to reflect upon the estimate of the trader before concluding the contract. Purchases made during an excursion organised by the trader during which the products acquired are promoted and offered for sale should be considered as off-premises contracts.

(22) Business premises should include premises in whatever form (such as shops, stalls or lorries) which serve as a permanent or usual place of business for the trader. Market stalls and fair stands should be treated as business premises if they fulfil this condition. Retail premises where the trader carries out his activity on a seasonal basis, for instance during the tourist season at a ski or beach resort, should be considered as business premises as the trader carries out his activity in those premises on a usual basis. Spaces accessible to the public, such as streets, shopping malls, beaches, sports facilities and public transport, which the trader uses on an exceptional basis for his business activities as well as private homes or workplaces should not be regarded as business premises. The business premises of a person acting in the name or on behalf of the trader as defined in this Directive should be considered as business premises within the meaning of this Directive.

(23) Durable media should enable the consumer to store the information for as long as it is necessary for him to protect his interests stemming from his relationship with the trader. Such media should include in particular paper, USB sticks, CD-ROMs, DVDs, memory cards or the hard disks of computers as well as e-mails.

(24) A public auction implies that traders and consumers attend or are given the possibility to attend the auction in person. The goods or services are offered by the trader to the consumer through a bidding procedure authorised by law in some Member States, to offer goods or services at public sale. The successful bidder is bound to purchase the goods or services. The use of online platforms for auction purposes which are at the disposal of consumers and traders should not be considered as a public auction within the meaning of this Directive.

(25) Contracts related to district heating should be covered by this Directive, similarly to the contracts for the supply of water, gas or electricity. District heating refers to 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.

(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 already 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 at national level. 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 and 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 provided in assisted 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 [1] 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 nurse responsible for general care, 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 [2] 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 cost 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

[1] OJ L 88, 4.4.2011, p. 45.
[2] OJ L 255, 30.9.2005, p. 22.

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 (EEC, Euratom) No 1182/71 of 3 June 1971 determining the rules applicable to periods, dates and time limits [1] should apply to the calculation of the periods contained in this Directive. Therefore, all periods contained in this Directive should be understood to be expressed in calendar days. Where a period expressed in days is to be calculated from the moment at which an event occurs or an action takes place, the day during which that event occurs or that action takes place should not 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 termination or unenforceability of a contract or the possibility for the consumer to fulfil 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 proof of 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.

[1] OJ L 124, 8.6.1971, p. 1.

(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 filling 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) In the event that 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 the 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 contract law provisions.

(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 exercises his 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 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 rules provided 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 delivery of goods, including goods getting lost or damaged during transport and late or partial delivery. Therefore it is appropriate to clarify and harmonise the national rules as to when delivery should occur. The place and modalities of delivery and the rules concerning the determination of the conditions 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 acquire on his behalf the physical possession or control of the goods. The consumer should be considered to have control of the goods where he or a third party indicated by the consumer has access to the goods to use them as an owner, or the ability to resell the goods (for example, when he has received the keys or possession of the ownership documents).

(52) In the context of sales contracts, the delivery of goods can take place in various ways, 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 has failed 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 when the trader has refused to deliver the goods in an unequivocal statement. Neither should it apply in certain 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 fulfil 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 [1], 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 of 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) Persons or 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') [2] 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.

[1] OJ L 319, 5.12.2007, p. 1.

[2] OJ L 149, 11.6.2005, p. 22.

(61) 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) [1] already regulates unsolicited communications and provides for a high level of consumer protection. The corresponding provisions on the same issue contained in Directive 97/7/EC are therefore not needed.

(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 [2] 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 [3]. 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 [4], 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, craft or profession in relation to contracts covered by this Directive;

(3) '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 a set quantity;

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

[1] OJ L 201, 31.7.2002, p. 37.
[2] OJ L 95, 21.4.1993, p. 29.
[3] OJ L 171, 7.7.1999, p. 12.
[4] OJ C 321, 31.12.2003, p. 1.

(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; or

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

(9) 'business premises' means:

(a) any immovable retail premises where the trader carries out his activity on a permanent basis; or

(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 supplied in digital form;

(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.

Article 3

Scope

1. This Directive shall apply, under the conditions and to the extent set out in its provisions, to any contract concluded between a trader and a consumer. It shall also apply to contracts for the supply of water, gas, electricity or district heating, including by public providers, to the extent that these commodities are provided on a contractual basis.

2. If any provision of this Directive conflicts with a provision of another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

3. This Directive shall not apply to contracts:

(a) for social services, including social housing, childcare and support of families and persons permanently or temporarily in need, including long-term care;

(b) for healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU, whether or not they are provided via healthcare facilities;

(c) for gambling, which involves wagering a stake with pecuniary value in games of chance, including lotteries, casino games and betting transactions;

(d) for financial services;

(e) for the creation, acquisition or transfer of immovable property or of rights in immovable property;

(f) for the construction of new buildings, the substantial conversion of existing buildings and for rental of accommodation for residential purposes;

(g) which fall within the scope of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours [1];

(h) which fall within the scope of Directive 2008/122/EC of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts [2];

(i) which, in accordance with the laws of Member States, are established by a public office-holder who has a statutory obligation to be independent and impartial and who must ensure, by providing comprehensive legal information, that the consumer only concludes the contract on the basis of careful legal consideration and with knowledge of its legal scope;

(j) for the supply of foodstuffs, beverages or other goods intended for current consumption in the household, and which are physically supplied by a trader on frequent and regular rounds to the consumer's home, residence or workplace;

(k) for passenger transport services, with the exception of Article 8(2) and Articles 19 and 22;

(l) concluded by means of automatic vending machines or automated commercial premises;

(m) concluded with telecommunications operators through public payphones for their use or concluded for the use of one single connection by telephone, Internet or fax established by a consumer.

4. Member States may decide not to apply this Directive or not to maintain or introduce corresponding national provisions to off-premises contracts for which the payment to be made by the consumer does not exceed EUR 50. Member States may define a lower value in their national legislation.

5. This Directive shall not affect national general contract law such as the rules on the validity, formation or effect of a contract, in so far as general contract law aspects are not regulated in this Directive.

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 manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges or, where those charges 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;

[1] OJ L 158, 23.6.1990, p. 59.
[2] OJ L 33, 3.2.2009, p. 10.

(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 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 (h), (i) and (j) of paragraph 1 may be provided by means of the model instructions on withdrawal set out in Annex I(A). The trader shall have fulfilled the information requirements laid down in points (h), (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 (i) 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), (h) 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 to 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 the last good;

(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 (h) 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.

Member States shall not provide for any formal requirements applicable to the model withdrawal form other than those set out in Annex I(B).

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 has expressly agreed otherwise and provided that the consumer does not incur any fees as a result of such reimbursement.

2. Notwithstanding paragraph 1, the trader shall not be required to reimburse the supplementary costs, if the consumer has expressly opted for a type of delivery other than the least expensive type of standard delivery offered by the trader.

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 to 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.

Article 15

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 [1], 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 in 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.

[1] OJ L 133, 22.5.2008, p. 66.

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 fulfil 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 of or 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(3), 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

Directive 85/577/EEC and Directive 97/7/EC, as amended by Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services [1] and by Directives 2005/29/EC and 2007/64/EC, are repealed as of 13 June 2014.

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 II.

[1] OJ L 271, 9.10.2002, p. 16.

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	*For the Council*
The President	*The President*
J. BUZEK	M. DOWGIELEWICZ

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 [1].

To exercise the right of withdrawal, you must inform us ([2]) 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. [3]

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. [4]

[5]

[6]

Instructions for completion:

[1.] 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 acquires, 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 acquires, 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 acquires, 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 acquires, physical possession of the first good.'.

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

[3.] 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.'.

[4.] 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.'.

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

(a) insert:

— 'We will collect the goods.'; or,

— 'You shall send back the goods or hand them over to us or … [insert the name and geographical address, where applicable, of the person authorised by you to receive the goods], without undue delay and in any event not later than 14 days from the day on which you communicate your withdrawal from this contract to us. The deadline is met if you send back the goods before the period of 14 days has expired.'

(b) insert:

— 'We will bear the cost of returning the goods.',

— 'You will have to bear the direct cost of returning the goods.',

— If, in a distance contract, you do not offer to bear the cost of returning the goods and the goods, by their nature, cannot normally be returned by post: 'You will have to bear the direct cost of returning the goods, … EUR [insert the amount].'; or if the cost of returning the goods cannot reasonably be calculated in advance: 'You will have to bear the direct cost of returning the goods. The cost is estimated at a maximum of approximately … EUR [insert the amount].'; or

— If, in an off-premises contract, the goods, by their nature, cannot normally be returned by post and have been delivered to the consumer's home at the time of the conclusion of the contract: 'We will collect the goods at our own expense.'; and,

(c) insert 'You are only liable for any diminished value of the goods resulting from the handling other than what is necessary to establish the nature, characteristics and functioning of the goods.'

6. In the case of a contract for the provision 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, insert the following: 'If you requested to begin the performance of services or the supply of water/gas/electricity/district heating [delete where inapplicable] during the withdrawal period, you shall pay us an amount which is in proportion to what has been provided until you have communicated us your withdrawal from this contract, in comparison with the full coverage of the contract.'.

B. Model withdrawal form

(complete and return this form only if you wish to withdraw from the contract)

— To [here the trader's name, geographical address and, where available, his fax number and e-mail address are to be inserted by the trader]:

— I/We (*) hereby give notice that I/We (*) withdraw from my/our (*) contract of sale of the following goods (*)/for the provision of the following service (*),

— Ordered on (*)/received on (*),

— Name of consumer(s),

— Address of consumer(s),

— Signature of consumer(s) (only if this form is notified on paper),

— Date

(*) Delete as appropriate.

ANNEX II

Correlation table

Directive 85/577/EEC	Directive 97/7/EC	This Directive
Article 1		Article 3 read in conjunction with Article 2, points 8 and 9, and Article 16, point (h)
	Article 1	Article 1 read in conjunction with Article 2, point 7
Article 2		Article 2, points 1 and 2
	Article 2, point 1	Article 2, point 7
	Article 2, point 2	Article 2, point 1
	Article 2, point 3	Article 2, point 2
	Article 2, point 4, first sentence	Article 2, point 7
	Article 2, point 4, second sentence	—
	Article 2, point 5	—
Article 3(1)		Article 3(4)
Article 3(2), point (a)		Article 3(3), points (e) and (f)
Article 3(2), point (b)		Article 3(3), point (j)
Article 3(2), point (c)		—
Article 3(2), point (d)		Article 3(3), point (d)
Article 3(2), point (e)		Article 3(3), point (d)
Article 3(3)		—
	Article 3(1), first indent	Article 3(3), point (d)
	Article 3(1), second indent	Article 3(3), point (l)
	Article 3(1), third indent	Article 3(3), point (m)
	Article 3(1), fourth indent	Article 3(3), points (e) and (f)
	Article 3(1), fifth indent	Article 6(3) and Article 16, point (k) read in conjunction with Article 2, point 13
	Article 3(2), first indent	Article 3(3), point (j)
	Article 3(2), second indent	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)
Article 4, first sentence		Article 6(1), points (b), (c) and (h), and Article 7(1) and (2)
Article 4, second sentence		Article 6(1), point a and Article 7(1)
Article 4, third sentence		Article 6(1)
Article 4, fourth sentence		Article 10
	Article 4(1), point (a)	Article 6(1), points (b) and (c)
	Article 4(1), point (b)	Article 6(1), point (a)

Directive 85/577/EEC	Directive 97/7/EC	This Directive
	Article 4(1), point (c)	Article 6(1), point (e)
	Article 4(1), point (d)	Article 6(1), point (e)
	Article 4(1), point (e)	Article 6(1), point (g)
	Article 4(1), point (f)	Article 6(1), point (h)
	Article 4(1), point (g)	Article 6(1), point (f)
	Article 4(1), point (h)	—
	Article 4(1), point (i)	Article 6(1), points (o) and (p)
	Article 4(2)	Article 6(1) read in conjunction with Article 8(1), (2) and (4)
	Article 4(3)	Article 8(5)
	Article 5(1)	Article 8(7)
	Article 5(2)	Article 3(3), point m
	Article 6(1)	Article 9(1) and (2), Article 10, Article 13(2), Article 14
	Article 6(2)	Article 13 and Article 14(1), second and third subparagraphs
	Article 6(3), first indent	Article 16, point (a)
	Article 6(3), second indent	Article 16, point (b)
	Article 6(3), third indent	Article 16, point (c) and (d)
	Article 6(3), fourth indent	Article 16, point (i)
	Article 6(3), fifth indent	Article 16, point (j)
	Article 6(3), sixth indent	Article 3(3), point (c)
	Article 6(4)	Article 15
	Article 7(1)	Article 18(1) (for sales contracts)
	Article 7(2)	Article 18(2), (3) and (4)
	Article 7(3)	—
	Article 8	—
	Article 9	Article 27
	Article 10	— (but see Article 13 of Directive 2002/58/EC)
	Article 11(1)	Article 23(1)
	Article 11(2)	Article 23(2)
	Article 11(3), point (a)	Article 6(9) for the burden of proof concerning pre-contractual information; for the rest: –
	Article 11(3), point (b)	Article 24(1)
	Article 11(4)	—
	Article 12(1)	Article 25
	Article 12(2)	—
	Article 13	Article 3(2)
	Article 14	Article 4

Directive 85/577/EEC	Directive 97/7/EC	This Directive
	Article 15(1)	Article 28(1)
	Article 15(2)	Article 28(1)
	Article 15(3)	Article 28(1)
	Article 15(4)	Article 30
	Article 16	Article 26
	Article 17	—
	Article 18	Article 34
	Article 19	Article 35
Article 5(1)		Articles 9 and 11
Article 5(2)		Article 12
Article 6		Article 25
Article 7		Articles 13, 14 and 15
Article 8		Article 4

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 consumer protection laws (the Regulation on consumer protection cooperation) [1]	To be construed as a reference to
Paragraphs 2 and 11	This Directive

[1] OJ L 364, 9.12.2004, p. 1.