Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance)

DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2009

amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

(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)],

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

Having regard to the opinion of the European Data Protection Supervisor[(3)],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[(4)],

Whereas:

(1) The functioning of the five directives comprising the existing regulatory framework for electronic communications networks and services (Directive 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)[(5)], Directive 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)[(6)], Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[(7)], Directive 2002/22/EC (Universal Service Directive)[(8)] and Directive 2002/58/EC (Directive on privacy and electronic communications)[(9)] (together referred to as 'the Framework Directive and the Specific Directives')) is subject to periodic review by the

Commission, with a view, in particular, to determining the need for modification in the light of technological and market developments.

(2) In that regard, the Commission presented its findings in its Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of 29 June 2006 on the review of the EU regulatory framework for electronic communications networks and services.

(3) The reform of the EU regulatory framework for electronic communications networks and services, including the reinforcement of provisions for end-users with disabilities, represents a key step towards simultaneously achieving a Single European Information Space and an inclusive information society. These objectives are included in the strategic framework for the development of the information society as described in the Commission Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of 1 June 2005 entitled 'i2010 – A European Information Society for growth and employment'.

(4) A fundamental requirement of universal service is to provide users on request with a connection to the public communications network at a fixed location and at an affordable price. The requirement is for the provision of local, national and international telephone calls, facsimile communications and data services, the provision of which may be restricted by Member States to the end-user's primary location or residence. There should be no constraints on the technical means by which this is provided, allowing for wired or wireless technologies, nor any constraints on which operators provide part or all of universal service obligations.

(5) Data connections to the public communications network at a fixed location should be capable of supporting data communications at rates sufficient for access to online services such as those provided via the public Internet. The speed of Internet access experienced by a given user may depend on a number of factors, including the provider(s) of Internet connectivity as well as the given application for which a connection is being used. The data rate that can be supported by a connection to the public communications network depends on the capabilities of the subscriber's terminal equipment as well as the connection. For this reason, it is not appropriate to mandate a specific data or bit rate at Community level. Flexibility is required to allow Member States to take measures, where necessary, to ensure that a data connection is capable of supporting satisfactory data rates which are sufficient to permit functional Internet access, as defined by the Member States, taking due account of specific circumstances in national markets, for instance the prevailing bandwidth used by the majority of subscribers in that Member State, and technological feasibility, provided that these measures seek to minimise market distortion. Where such measures result in an unfair burden on a designated undertaking, taking due account of the costs and revenues as well as the intangible benefits resulting from the provision of the services concerned, this may be included in any net cost calculation of universal obligations. Alternative financing of underlying network infrastructure, involving Community funding or national measures in accordance with Community law, may also be implemented.

(6) This is without prejudice to the need for the Commission to conduct a review of the universal service obligations, which may include the financing of such obligations, in accordance with Article 15 of Directive 2002/22/EC (Universal Service Directive), and, if appropriate, to present proposals for reform to meet public interest objectives.

(7) For the sake of clarity and simplicity, this Directive only deals with amendments to Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications).

(8) Without prejudice to 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[(10)], and in particular the disability requirements laid down in Article 3(3)(f) thereof, certain aspects of terminal equipment, including consumer premises equipment intended for disabled end-users, whether their special needs are due to disability or related to ageing, should be brought within the scope of Directive 2002/22/EC (Universal Service Directive) in order to facilitate access to networks and the use of services. Such equipment currently includes receive-only radio and television terminal equipment as well as special terminal devices for hearing-impaired end-users.

(9) Member States should introduce measures to promote the creation of a market for widely available products and services incorporating facilities for disabled end-users. This can be achieved, inter alia, by referring to European standards, introducing electronic accessibility (eAccessibility) requirements for public procurement procedures and calls for tender relating to the provision of services, and by implementing legislation upholding the rights of disabled end-users.

(10) When an undertaking designated to provide universal service, as identified in Article 4 of Directive 2002/22/EC (Universal Service Directive), chooses to dispose of a substantial part, viewed in light of its universal service obligation, or all, of its local access network assets in the national territory to a separate legal entity under different ultimate ownership, the national regulatory authority should assess the effects of the transaction in order to ensure the continuity of universal service obligations in all or parts of the national territory. To this end, the national regulatory authority which imposed the universal service obligations should be informed by the undertaking in advance of the disposal. The assessment of the national regulatory authority should not prejudice the completion of the transaction.

(11) Technological developments have led to substantial reductions in the number of public pay telephones. In order to ensure technological neutrality and continued access by the public to voice telephony, national regulatory authorities should be able to impose obligations on undertakings to ensure not only that public pay telephones are provided to meet the reasonable needs of end-users, but also that alternative public voice telephony access points are provided for that purpose, if appropriate.

(12) Equivalence in disabled end-users' access to services should be guaranteed to the level available to other end-users. To this end, access should be functionally equivalent, such

that disabled end-users benefit from the same usability of services as other end-users, but by different means.

(13) Definitions need to be adjusted so as to conform to the principle of technology neutrality and to keep pace with technological development. In particular, conditions for the provision of a service should be separated from the actual definitional elements of a publicly available telephone service, i.e. an electronic communications service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan, whether such a service is based on circuit switching or packet switching technology. It is the nature of such a service that it is bidirectional, enabling both the parties to communicate. A service which does not fulfil all these conditions, such as for example a 'click-through' application on a customer service website, is not a publicly available telephone service. Publicly available telephone services also include means of communication specifically intended for disabled end-users using text relay or total conversation services.

(14) It is necessary to clarify that the indirect provision of services could include situations where originating is made via carrier selection or pre-selection or where a service provider resells or re-brands publicly available telephone services provided by another undertaking.

(15) As a result of technological and market evolution, networks are increasingly moving to 'Internet Protocol' (IP) technology, and consumers are increasingly able to choose between a range of competing voice service providers. Therefore, Member States should be able to separate universal service obligations concerning the provision of a connection to the public communications network at a fixed location from the provision of a publicly available telephone service. Such separation should not affect the scope of universal service obligations defined and reviewed at Community level.

(16) In accordance with the principle of subsidiarity, it is for the Member States to decide on the basis of objective criteria which undertakings are designated as universal service providers, where appropriate taking into account the ability and the willingness of undertakings to accept all or part of the universal service obligations. This does not preclude that Member States may include, in the designation process, specific conditions justified on grounds of efficiency, including, inter alia, grouping geographical areas or components or setting minimum periods for the designation.

(17) National regulatory authorities should be able to monitor the evolution and level of retail tariffs for services that fall under the scope of universal service obligations, even where a Member State has not yet designated an undertaking to provide universal service. In such a case, the monitoring should be carried out in such a way that it would not represent an excessive administrative burden for either national regulatory authorities or undertakings providing such service.

(18) Redundant obligations designed to facilitate the transition from the regulatory framework of 1998 to that of 2002 should be deleted, together with other provisions that overlap with and duplicate those laid down in Directive 2002/21/EC (Framework Directive).

(19) The requirement to provide a minimum set of leased lines at retail level, which was necessary to ensure the continued application of provisions of the regulatory framework of 1998 in the field of leased lines, which was not sufficiently competitive at the time the 2002 framework entered into force, is no longer necessary and should be repealed.

(20) To continue to impose carrier selection and carrier pre-selection directly in Community legislation could hamper technological progress. These remedies should rather be imposed by national regulatory authorities as a result of market analysis carried out in accordance with the procedures set out in Directive 2002/21/EC (Framework Directive) and through the obligations referred to in Article 12 of Directive 2002/19/EC (Access Directive).

(21) Provisions on contracts should apply not only to consumers but also to other end-users, primarily micro enterprises and small and medium-sized enterprises (SMEs), which may prefer a contract adapted to consumer needs. To avoid unnecessary administrative burdens for providers and the complexity related to the definition of SMEs, the provisions on contracts should not apply automatically to those other end-users, but only where they so request. Member States should take appropriate measures to promote awareness amongst SMEs of this possibility.

(22) As a consequence of technological developments, other types of identifiers may be used in the future, in addition to ordinary forms of numbering identification.

(23) Providers of electronic communications services that allow calls should ensure that their customers are adequately informed as to whether or not access to emergency services is provided and of any limitation on service (such as a limitation on the provision of caller location information or the routing of emergency calls). Such providers should also provide their customers with clear and transparent information in the initial contract and in the event of any change in the access provision, for example in billing information. This information should include any limitations on territorial coverage, on the basis of the planned technical operating parameters of the service and the available infrastructure. Where the service is not provided over a switched telephony network, the information should also include the level of reliability of the access and of caller location information compared to a service that is provided over a switched telephony network, taking into account current technology and quality standards, as well as any quality of service parameters specified under Directive 2002/22/EC (Universal Service Directive).

(24) With respect to terminal equipment, the customer contract should specify any restrictions imposed by the provider on the use of the equipment, such as by way of ‘SIM-locking’ mobile devices, if such restrictions are not prohibited under national legislation, and any charges due on termination of the contract, whether before or on the agreed expiry date, including any cost imposed in order to retain the equipment.

(25) Without imposing any obligation on the provider to take action over and above what is required under Community law, the customer contract should also specify the type of action, if any, the provider might take in case of security or integrity incidents, threats or vulnerabilities.

(26) In order to address public interest issues with respect to the use of communications services and to encourage protection of the rights and freedoms of others, the relevant national authorities should be able to produce and have disseminated, with the aid of providers, public interest information related to the use of such services. This could include public interest information regarding copyright infringement, other unlawful uses and the dissemination of harmful content, and advice and means of protection against risks to personal security, which may for example arise from disclosure of personal information in certain circumstances, as well as risks to privacy and personal data, and the availability of easy-to-use and configurable software or software options allowing protection for children or vulnerable persons. The information could be coordinated by way of the cooperation procedure established in Article 33(3) of Directive 2002/22/EC (Universal Service Directive). Such public interest information should be updated whenever necessary and should be presented in easily comprehensible printed and electronic formats, as determined by each Member State, and on national public authority websites. National regulatory authorities should be able to oblige providers to disseminate this standardised information to all their customers in a manner deemed appropriate by the national regulatory authorities. When required by Member States, the information should also be included in contracts. Dissemination of such information should however not impose an excessive burden on undertakings. Member States should require this dissemination by the means used by undertakings in communications with subscribers made in the ordinary course of business.

(27) The right of subscribers to withdraw from their contracts without penalty refers to modifications in contractual conditions which are imposed by the providers of electronic communications networks and/or services.

(28) End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes, without prejudice to the need to preserve the integrity and security of networks and services. A competitive market will provide users with a wide choice of content, applications and services. National regulatory authorities should promote users' ability to access and distribute information and to run applications and services of their choice, as provided for in Article 8 of Directive 2002/21/EC (Framework Directive). Given the increasing importance of electronic communications for consumers and businesses, users should in any case be fully informed of any limiting conditions imposed on the use of electronic communications services by the service and/or network provider. Such information should, at the option of the provider, specify the type of content, application or service concerned, individual applications or services, or both. Depending on the technology used and the type of limitation, such limitations may require user consent under Directive 2002/58/EC (Directive on privacy and electronic communications).

(29) Directive 2002/22/EC (Universal Service Directive) neither mandates nor prohibits conditions imposed by providers, in accordance with national law, limiting end-users' access to and/or use of services and applications, but lays down an obligation to provide information regarding such conditions. Member States wishing to implement measures

regarding end-users' access to and/or use of services and applications must respect the fundamental rights of citizens, including in relation to privacy and due process, and any such measures should take full account of policy goals defined at Community level, such as furthering the development of the Community information society.

(30) Directive 2002/22/EC (Universal Service Directive) does not require providers to monitor information transmitted over their networks or to bring legal proceedings against their customers on grounds of such information, nor does it make providers liable for that information. Responsibility for punitive action or criminal prosecution is a matter for national law, respecting fundamental rights and freedoms, including the right to due process.

(31) In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful. The Framework Directive and the Specific Directives are without prejudice to 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)[(11)], which, inter alia, contains a 'mere conduit' rule for intermediary service providers, as defined therein.

(32) The availability of transparent, up-to-date and comparable information on offers and services is a key element for consumers in competitive markets where several providers offer services. End-users and consumers of electronic communications services should be able to easily compare the prices of various services offered on the market based on information published in an easily accessible form. In order to allow them to make price comparisons easily, national regulatory authorities should be able to require from undertakings providing electronic communications networks and/or services greater transparency as regards information (including tariffs, consumption patterns and other relevant statistics) and to ensure that third parties have the right to use, without charge, publicly available information published by such undertakings. National regulatory authorities should also be able to make price guides available, in particular where the market has not provided them free of charge or at a reasonable price. Undertakings should not be entitled to any remuneration for the use of information where it has already been published and thus belongs in the public domain. In addition, end-users and consumers should be adequately informed of the price and the type of service offered before they purchase a service, in particular if a freephone number is subject to additional charges. National regulatory authorities should be able to require that such information is provided generally, and, for certain categories of services determined by them, immediately prior to connecting the call, unless otherwise provided for by national law. When determining the categories of call requiring pricing information prior to connection, national regulatory authorities should take due account of the nature of the service, the pricing conditions which apply to it and whether it is offered by a provider who is not a provider of electronic communications services. Without prejudice to Directive 2000/31/EC (Directive on electronic commerce), undertakings

should also, if required by Member States, provide subscribers with public interest information produced by the relevant public authorities regarding, inter alia, the most common infringements and their legal consequences.

(33) Customers should be informed of their rights with respect to the use of their personal information in subscriber directories and in particular of the purpose or purposes of such directories, as well as their right, free of charge, not to be included in a public subscriber directory, as provided for in Directive 2002/58/EC (Directive on privacy and electronic communications). Customers should also be informed of systems which allow information to be included in the directory database but which do not disclose such information to users of directory services.

(34) A competitive market should ensure that end-users enjoy the quality of service they require, but in particular cases it may be necessary to ensure that public communications networks attain minimum quality levels so as to prevent degradation of service, the blocking of access and the slowing of traffic over networks. In order to meet quality of service requirements, operators may use procedures to measure and shape traffic on a network link so as to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance. Those procedures should be subject to scrutiny by the national regulatory authorities, acting in accordance with the Framework Directive and the Specific Directives and in particular by addressing discriminatory behaviour, in order to ensure that they do not restrict competition. If appropriate, national regulatory authorities may also impose minimum quality of service requirements on undertakings providing public communications networks to ensure that services and applications dependent on the network are delivered at a minimum quality standard, subject to examination by the Commission. National regulatory authorities should be empowered to take action to address degradation of service, including the hindering or slowing down of traffic, to the detriment of consumers. However, since inconsistent remedies can impair the functioning of the internal market, the Commission should assess any requirements intended to be set by national regulatory authorities for possible regulatory intervention across the Community and, if necessary, issue comments or recommendations in order to achieve consistent application.

(35) In future IP networks, where provision of a service may be separated from provision of the network, Member States should determine the most appropriate steps to be taken to ensure the availability of publicly available telephone services provided using public communications networks and uninterrupted access to emergency services in the event of catastrophic network breakdown or in cases of force majeure, taking into account the priorities of different types of subscriber and technical limitations.

(36) In order to ensure that disabled end-users benefit from competition and the choice of service providers enjoyed by the majority of end-users, relevant national authorities should specify, where appropriate and in light of national conditions, consumer protection requirements to be met by undertakings providing publicly available electronic communications services. Such requirements may include, in particular, that undertakings ensure that disabled end-users take advantage of their services on

equivalent terms and conditions, including prices and tariffs, as those offered to their other end-users, irrespective of any additional costs incurred by them. Other requirements may relate to wholesale arrangements between undertakings.

(37) Operator assistance services cover a range of different services for end-users. The provision of such services should be left to commercial negotiations between providers of public communications networks and operator assistance services, as is the case for any other customer support service, and it is not necessary to continue to mandate their provision. The corresponding obligation should therefore be repealed.

(38) Directory enquiry services should be, and frequently are, provided under competitive market conditions, pursuant to Article 5 of Commission Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communications networks and services[(12)]. Wholesale measures ensuring the inclusion of end-user data (both fixed and mobile) in databases should comply with the safeguards for the protection of personal data, including Article 12 of Directive 2002/58/EC (Directive on privacy and electronic communications). The cost-oriented supply of that data to service providers, with the possibility for Member States to establish a centralised mechanism for providing comprehensive aggregated information to directory providers, and the provision of network access under reasonable and transparent conditions, should be put in place in order to ensure that end-users benefit fully from competition, with the ultimate aim of enabling the removal of retail regulation from these services and the provision of offers of directory services under reasonable and transparent conditions.

(39) End-users should be able to call and access the emergency services using any telephone service capable of originating voice calls through a number or numbers in national telephone numbering plans. Member States that use national emergency numbers besides ‘112’ may impose on undertakings similar obligations for access to such national emergency numbers. Emergency authorities should be able to handle and answer calls to the number ‘112’ at least as expeditiously and effectively as calls to national emergency numbers. It is important to increase awareness of ‘112’ in order to improve the level of protection and security of citizens travelling in the European Union. To this end, citizens should be made fully aware, when travelling in any Member State, in particular through information provided in international bus terminals, train stations, ports or airports and in telephone directories, payphone kiosks, subscriber and billing material, that ‘112’ can be used as a single emergency number throughout the Community. This is primarily the responsibility of the Member States, but the Commission should continue both to support and to supplement initiatives of the Member States to heighten awareness of ‘112’ and periodically to evaluate the public’s awareness of it. The obligation to provide caller location information should be strengthened so as to increase the protection of citizens. In particular, undertakings should make caller location information available to emergency services as soon as the call reaches that service independently of the technology used. In order to respond to technological developments, including those leading to increasingly accurate caller location information, the Commission should be empowered to adopt technical implementing measures to ensure effective access to ‘112’ services in the Community

for the benefit of citizens. Such measures should be without prejudice to the organisation of emergency services of Member States.

(40) Member States should ensure that undertakings providing end-users with an electronic communications service designed for originating calls through a number or numbers in a national telephone numbering plan provide reliable and accurate access to emergency services, taking into account national specifications and criteria. Network-independent undertakings may not have control over networks and may not be able to ensure that emergency calls made through their service are routed with the same reliability, as they may not be able to guarantee service availability, given that problems related to infrastructure are not under their control. For network-independent undertakings, caller location information may not always be technically feasible. Once internationally-recognised standards ensuring accurate and reliable routing and connection to the emergency services are in place, network-independent undertakings should also fulfil the obligations related to caller location information at a level comparable to that required of other undertakings.

(41) Member States should take specific measures to ensure that emergency services, including '112', are equally accessible to disabled end-users, in particular deaf, hearing-impaired, speech-impaired and deaf-blind users. This could involve the provision of special terminal devices for hearing-impaired users, text relay services, or other specific equipment.

(42) Development of the international code '3883' (the European Telephony Numbering Space (ETNS)) is currently hindered by insufficient awareness, overly bureaucratic procedural requirements and, in consequence, lack of demand. In order to encourage the development of ETNS, the Member States to which the International Telecommunications Union has assigned the international code '3883' should, following the example of the implementation of the '.eu' top-level domain, delegate responsibility for its management, number assignment and promotion to an existing separate organisation, designated by the Commission on the basis of an open, transparent and non-discriminatory selection procedure. That organisation should also have the task of developing proposals for public service applications using ETNS for common European services, such as a common number for reporting thefts of mobile terminals.

(43) Considering the particular aspects related to reporting missing children and the currently limited availability of such a service, Member States should not only reserve a number, but also make every effort to ensure that a service for reporting missing children is actually available in their territories under the number '116000', without delay. To that end, Member States should, if appropriate, inter alia, organise tendering procedures in order to invite interested parties to provide that service.

(44) Voice calls remain the most robust and reliable form of access to emergency services. Other means of contact, such as text messaging, may be less reliable and may suffer from lack of immediacy. Member States should, however, if they deem it appropriate, be free to promote the development and implementation of other means of access to emergency services which are capable of ensuring access equivalent to voice calls.

(45) Pursuant to its Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with '116' for harmonised numbers for harmonised services of social value[(13)], the Commission has asked Member States to reserve numbers in the '116' numbering range for certain services of social value. The appropriate provisions of that Decision should be reflected in Directive 2002/22/EC (Universal Service Directive) in order to integrate them more firmly into the regulatory framework for electronic communications networks and services and to facilitate access by disabled end-users.

(46) A single market implies that end-users are able to access all numbers included in the national numbering plans of other Member States and to access services using non-geographic numbers within the Community, including, among others, freephone and premium rate numbers. End-users should also be able to access numbers from the European Telephone Numbering Space (ETNS) and Universal International Freephone Numbers (UIFN). Cross-border access to numbering resources and associated services should not be prevented, except in objectively justified cases, for example to combat fraud or abuse (e.g. in connection with certain premium-rate services), when the number is defined as having a national scope only (e.g. a national short code) or when it is technically or economically unfeasible. Users should be fully informed in advance and in a clear manner of any charges applicable to freephone numbers, such as international call charges for numbers accessible through standard international dialling codes.

(47) In order to take full advantage of the competitive environment, consumers should be able to make informed choices and to change providers when it is in their interests. It is essential to ensure that they can do so without being hindered by legal, technical or practical obstacles, including contractual conditions, procedures, charges and so on. This does not preclude the imposition of reasonable minimum contractual periods in consumer contracts. Number portability is a key facilitator of consumer choice and effective competition in competitive markets for electronic communications and should be implemented with the minimum delay, so that the number is functionally activated within one working day and the user does not experience a loss of service lasting longer than one working day. Competent national authorities may prescribe the global process of the porting of numbers, taking into account national provisions on contracts and technological developments. Experience in certain Member States has shown that there is a risk of consumers being switched to another provider without having given their consent. While that is a matter that should primarily be addressed by law enforcement authorities, Member States should be able to impose such minimum proportionate measures regarding the switching process, including appropriate sanctions, as are necessary to minimise such risks, and to ensure that consumers are protected throughout the switching process without making the process less attractive for them.

(48) Legal 'must-carry' obligations may be applied to specified radio and television broadcast channels and complementary services supplied by a specified media service provider. Member States should provide a clear justification for the 'must carry' obligations in their national law so as to ensure that such obligations are transparent, proportionate and properly defined. In that regard, 'must carry' rules should be designed in a way which provides sufficient incentives for efficient investment in infrastructure.

'Must carry' rules should be periodically reviewed in order to keep them up-to-date with technological and market evolution and in order to ensure that they continue to be proportionate to the objectives to be achieved. Complementary services include, but are not limited to, services designed to improve accessibility for end-users with disabilities, such as videotext, subtitling, audio description and sign language.

(49) In order to overcome existing shortcomings in terms of consumer consultation and to appropriately address the interests of citizens, Member States should put in place an appropriate consultation mechanism. Such a mechanism could take the form of a body which would, independently of the national regulatory authority and service providers, carry out research into consumer-related issues, such as consumer behaviour and mechanisms for changing suppliers, and which would operate in a transparent manner and contribute to the existing mechanisms for stakeholder consultation. Furthermore, a mechanism could be established for the purpose of enabling appropriate cooperation on issues relating to the promotion of lawful content. Any cooperation procedures agreed pursuant to such a mechanism should, however, not allow for the systematic surveillance of Internet usage.

(50) Universal service obligations imposed on an undertaking designated as having universal service obligations should be notified to the Commission.

(51) Directive 2002/58/EC (Directive on privacy and electronic communications) provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right to privacy and the right to confidentiality, with respect to the processing of personal data in the electronic communications sector, and to ensure the free movement of such data and of electronic communications equipment and services in the Community. Where measures aiming to ensure that terminal equipment is constructed so as to safeguard the protection of personal data and privacy are adopted pursuant to Directive 1999/5/EC or Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications[(14)], such measures should respect the principle of technology neutrality.

(52) Developments concerning the use of IP addresses should be followed closely, taking into consideration the work already done by, among others, 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 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[(15)], and in the light of such proposals as may be appropriate.

(53) The processing of traffic data to the extent strictly necessary 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 data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/

EC. 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.

(54) The liberalisation of electronic communications networks and services markets and rapid technological development have combined to boost competition and economic growth and resulted in a rich diversity of end-user services accessible via public electronic communications networks. It is necessary to ensure that consumers and users are afforded the same level of protection of privacy and personal data, regardless of the technology used to deliver a particular service.

(55) In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, Directive 2002/58/EC (Directive on privacy and electronic communications) focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks.

(56) Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens. To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply.

(57) The provider of a publicly available electronic communications service should take appropriate technical and organisational measures to ensure the security of its services. Without prejudice to Directive 95/46/EC, such measures should ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, and that the personal data stored or transmitted, as well as the network and services, are protected. Moreover, a security policy with respect to the processing of personal data should be established in order to identify vulnerabilities in the system, and monitoring and preventive, corrective and mitigating action should be regularly carried out.

(58) The competent national authorities should promote the interests of citizens by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory

of personal data breaches to enable further analysis and evaluation by the competent national authorities.

(59) Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against, for example, loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures. The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.

(60) Competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services.

(61) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned. Therefore, as soon as the provider of publicly available electronic communications services becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The subscribers or individuals whose data and privacy could be adversely affected by the breach should be notified without delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned.

(62) When implementing measures transposing Directive 2002/58/EC (Directive on privacy and electronic communications), the authorities and courts of the Member States should not only interpret their national law in a manner consistent with that Directive, but should also ensure that they do not rely on an interpretation of it which would conflict

with fundamental rights or general principles of Community law, such as the principle of proportionality.

(63) Provision should be made for the adoption of technical implementing measures concerning the circumstances, format and procedures applicable to information and notification requirements in order to achieve an adequate level of privacy protection and security of personal data transmitted or processed in connection with the use of electronic communications networks in the internal market.

(64) 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 the 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 in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(65) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.

(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.

(67) Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.

(68) Electronic communications service providers make substantial investments in order to combat unsolicited commercial communications (spam). They are also in a better position than end-users in that they possess the knowledge and resources necessary to detect and identify spammers. E-mail service providers and other service providers should therefore be able to initiate legal action against spammers, and thus defend the interests of their customers, as part of their own legitimate business interests.

(69) The need to ensure an adequate level of protection of privacy and personal data transmitted and processed in connection with the use of electronic communications networks in the Community calls for effective implementation and enforcement powers in order to provide adequate incentives for compliance. Competent national authorities and, where appropriate, other relevant national bodies should have sufficient powers and resources to investigate cases of non-compliance effectively, including powers to obtain any relevant information they might need, to decide on complaints and to impose sanctions in cases of non-compliance.

(70) The implementation and enforcement of the provisions of this Directive often require cooperation between the national regulatory authorities of two or more Member States, for example in combating cross-border spam and spyware. In order to ensure smooth and rapid cooperation in such cases, procedures relating for example to the quantity and format of information exchanged between authorities, or deadlines to be complied with, should be defined by the relevant national authorities, subject to examination by the Commission. Such procedures will also allow the resulting obligations of market actors to be harmonised, contributing to the creation of a level playing field in the Community.

(71) Cross-border cooperation and enforcement should be reinforced in line with existing Community cross-border enforcement mechanisms, such as that laid down in Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation)[(16)], by way of an amendment to that Regulation.

(72) The measures necessary for the implementation of Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) 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[(17)].

(73) In particular, the Commission should be empowered to adopt implementing measures on effective access to '112' services, as well as to adapt the Annexes to technical progress or changes in market demand. It should also be empowered to adopt implementing measures concerning information and notification requirements and security of processing. Since those measures are of general scope and are designed to amend non-essential elements of Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) by supplementing them with new non-essential elements, they must be adopted in accordance with the regulatory procedure with scrutiny provided for in Article 5a of Decision 1999/468/EC. Given that the conduct of the regulatory procedure with scrutiny within the normal time limits could, in certain exceptional situations, impede the timely adoption of implementing measures, the European Parliament, the Council

and the Commission should act speedily in order to ensure the timely adoption of those measures.

(74) When adopting implementing measures on security of processing, the Commission should consult all relevant European authorities and organisations (the European Network and Information Security Agency (ENISA), the European Data Protection Supervisor and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC), as well as all other relevant stakeholders, particularly in order to be informed of the best available technical and economic means of improving the implementation of Directive 2002/58/EC (Directive on privacy and electronic communications).

(75) Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) should therefore be amended accordingly.

(76) In accordance with point 34 of the Interinstitutional Agreement on better law-making[(18)], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) and the transposition measures, and to make them public,

HAVE ADOPTED THIS DIRECTIVE:

[F1 Article 1

[[F1 Amendments to Directive 2002/22/EC (Universal Service Directive)]

. . . . . .

Textual Amendments

F1 Deleted by Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance).

Article 2

Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)

Directive 2002/58/EC (Directive on privacy and electronic communications) is hereby amended as follows:

1) Article 1(1) shall be replaced by the following:

1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the

free movement of such data and of electronic communication equipment and services in the Community.;

2) Article 2 shall be amended as follows:

(a) point (c) shall be replaced by the following:

(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;;

(b) point (e) shall be deleted;

(c) **[**[X1]the following point shall be added:

(i) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.;**]**

3) Article 3 shall be replaced by the following:

Article 3

Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.;

4) Article 4 shall be amended as follows:

(a) the title shall be replaced by the following:

Security of processing;

(b) the following paragraph shall be inserted:

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,

— ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to

issue recommendations about best practices concerning the level of security which those measures should achieve.;

(c) the following paragraphs shall be added:

3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4 Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

5 In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt

technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).;

5) Article 5(3) shall be replaced by the following:

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.;

6) Article 6(3) shall be replaced by the following:

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.;

7) Article 13 shall be replaced by the following:

Article 13

Unsolicited communications

1 The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2 Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3 Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred

to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4 In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5 Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6 Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.;

8) the following Article shall be inserted:

Article 14a

Committee procedure

1 The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2 Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3 Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.;

9) in Article 15, the following paragraph shall be inserted:

1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.;

10) the following Article shall be inserted:

Article 15a

Implementation and enforcement

1 Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.

2 Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

3 Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4 The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.

The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures..

Editorial Information

X1 Substituted by Corrigendum to Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Official Journal of the European Union L 337 of 18 December 2009).

Article 3

Amendment to Regulation (EC) No 2006/2004

In the Annex to Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation), the following point shall be added:

17. 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): Article 13 (OJ L 201, 31.7.2002, p. 37)..

Article 4

Transposition

1 Member States shall adopt and publish by 25 May 2011 the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of those measures.

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. The methods of making such reference shall be laid down by the Member States.

2 Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 5

Entry into force

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

Article 6

Addressees

This Directive is addressed to the Member States.

[F1]ANNEX I

[F1. . . . . .]

ANNEX II

‘ANNEX VI

INTEROPERABILITY OF DIGITAL CONSUMER EQUIPMENT REFERRED TO IN ARTICLE 24

1. Common scrambling algorithm and free-to-air reception

All consumer equipment intended for the reception of conventional digital television signals (i.e. broadcasting via terrestrial, cable or satellite transmission which is primarily intended for fixed reception, such as DVB-T, DVB-C or DVB-S), for sale or rent or otherwise made available in the Community, capable of descrambling digital television signals, is to possess the capability to:

— allow the descrambling of such signals according to a common European scrambling algorithm as administered by a recognised European standards organisation, currently ETSI,

— display signals that have been transmitted in the clear provided that, in the event that such equipment is rented, the renter is in compliance with the relevant rental agreement.

2. Interoperability for analogue and digital television sets

Any analogue television set with an integral screen of visible diagonal greater than 42 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket, as standardised by a recognised European standards organisation, e.g. as given in the Cenelec EN 50 049-1:1997 standard, permitting simple connection of peripherals, especially additional decoders and digital receivers.

Any digital television set with an integral screen of visible diagonal greater than 30 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket (either standardised by, or conforming to a standard adopted by, a recognised European standards organisation, or conforming to an industry-wide specification) e.g. the DVB common interface connector, permitting simple connection of peripherals, and able to pass all the elements of a digital television signal, including information relating to interactive and conditionally accessed services.’

(**1**) OJ C 224, 30.8.2008, p. 50.

(**2**) OJ C 257, 9.10.2008, p. 51.

(**3**) OJ C 181, 18.7.2008, p. 1.

(**4**) Opinion of the European Parliament of 24 September 2008 (not yet published in the Official Journal), Council Common Position of 16 February 2009 (OJ C 103 E, 5.5.2009, p. 40), Position of the European Parliament of 6 May 2009 and Council Decision of 26 October 2009.

(**5**) OJ L 108, 24.4.2002, p. 7.

(**6**) OJ L 108, 24.4.2002, p. 21.

(**7**) OJ L 108, 24.4.2002, p. 33.

(**8**) OJ L 108, 24.4.2002, p. 51.

(**9**) OJ L 201, 31.7.2002, p. 37.

(**10**) OJ L 91, 7.4.1999, p. 10.

(**11**) OJ L 178, 17.7.2000, p. 1.

(**12**) OJ L 249, 17.9.2002, p. 21.

(**13**) OJ L 49, 17.2.2007, p. 30.

(**14**) OJ L 36, 7.2.1987, p. 31.

(**15**) OJ L 281, 23.11.1995, p. 31.

(**16**) OJ L 364, 9.12.2004, p. 1.

(**17**) OJ L 184, 17.7.1999, p. 23.

(**18**) OJ C 321, 31.12.2003, p. 1.