WORKING PARTY ON TELECOMMUNICATIONS AND INFORMATION SOCIETY 09/10/2008
Room document 70/08

Brussels, 6 October 2008

PRESIDENCY COMPROMISE PROPOSAL FOR THE

CONSOLIDATED VERSION OF THE PROPOSAL AMENDING DIRECTIVE 2002/58/EC (Privacy Directive)

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:

[for the Recitals common to this Directive and the Universal Service Directive, confer to the Universal Service Directive]

(27) 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. There is a need 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.

(30b) When implementing measures transposing Directive 2002/58/EC, 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 that Directive which would be in conflict with other fundamental rights or general principles of Community law, such as the principle of proportionality.

[for other recitals, see relevant Articles]

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope and aim

1. This Directive ~~**harmonises**~~ **provides for the harmonisation** of 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.

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[1].

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 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**~~ **electronic communications** service allowing two-way communication ~~in real time~~;

[1] LU suggests inserting "**natural or** legal persons".

(f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient**;**

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

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**, inlcuding public communications networks supporting data collection and identification devices.**

~~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.~~

(28) Technological progress allows the development of new applications based on devices for data collection and identification, which may be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFID) 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 benefits and thus make a powerful contribution to the internal market if their use is acceptable to citizens. To achieve that, it is necessary to ensure that ***all*** *the fundamental rights of individuals,* ~~***in particular***~~ ***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, including those on security, traffic and location data and on confidentiality, should apply.*

Article 4

Security of processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

3. In case of a personal data 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 by the provider of publicly available electronic communications service in the Community,~~ the provider of publicly available electronic communications services concerned shall, ~~without undue delay, notify the subscriber concerned and the national regulatory authority of such a breach.~~ assess the scope of the personal data breach, evaluate its seriousness and consider whether notification of the personal data breach to the competent national authority and subscriber concerned is necessary, taking into account the relevant rules set by the competent national authority in accordance with paragraph 3a.

When the personal data breach represents a serious risk for subscriber's privacy, the provider of publicly available electronic communications services concerned shall notify the competent national authority and the subscriber concerned of such a breach without undue delay.

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

(28b) 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 regular monitoring and preventive, corrective and mitigating action should be carried out.

(28c) Competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services.

(29) *A breach of security resulting in the loss or compromising personal data of an individual subscriber may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud. Therefore**, as soon as the provider of publicly available electronic communications service becomes aware that such breach has occurred it should assess the risks associated with it, e.g. by establishing the type of data affected by the breach (including their sensitivity, context and security measures in place), the cause and extent of the security breach, the number of subscribers affected, and the possible harm for subscribers as a result of the breach (e.g. identity theft, financial loss, loss of business or employment opportunities, physical harm).** The subscribers concerned by **~~such~~** security incidents **that could result in a serious risk to subscriber's privacy (e.g. identity theft or fraud, physical harm, significant humiliation or damage of reputation),** should be notified without delay **~~and informed~~** in order to be able to take the necessary precautions. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the users affected. **Notification of a security breach to a subscriber should not be required if the provider has demonstrated to the competent authority that it has implemented appropriate technological protection measures, and 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 authorized to access the data.***

(30) *National regulatory authorities should promote the interests of the citizens of the European Union by inter alia contributing to ensuring a high level of protection of personal data and privacy. To this end, they must have the necessary means to perform their duties, including comprehensive and reliable data about actual security incidents that have led to the personal data of individuals being compromised.*

3a. Member States shall ensure that the competent national authority is able to set detailed rules and, where necessary, issue instructions concerning the circumstances when the notification of personal data breaches by the provider of a publicly available electronic communications service is required, the format applicable to such notification as well as the manner in which the notification is done.

4. In order to ensure consistency in implementation of the measures referred to in paragraph 1, 2 and 3, the Commission may, following consultation with the European Network and Information Security Agency[2] ~~Electronic Communications Market Authority (hereinafter referred to as "the Authority")~~, the Article 29 Working Party and the European Data Protection Supervisor, adopt recommendations[3] ~~technical implementing measures~~ concerning *inter alia* the circumstances, format and procedures applicable to information and notification requirements referred to in 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). On imperative grounds of urgency, the Commission may use the urgency procedure referred to in Article 14a (3).~~

[2] FI and DE have a reserve on the reference to ENISA.
[3] DE suggests replacing "recommendations" by "guidelines".

(31) *Provision should be made for* ~~*implementing measures*~~ ***to establish a common set of requirements*** ~~*the Commission to adopt Recommendations on the means*~~ *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.*

(32) *In setting detailed rules concerning the format and procedures applicable to the notification of* ~~*security*~~ ***personal data*** *breaches, due consideration should be given to the circumstances of the breach, including whether or not the personal data had been protected by encryption or other means, 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.*

~~***(33) The Authority can contribute to the enhanced level of protection for personal data and privacy in the Community by, among other things, providing expertise and advice, promoting the exchange of best practices in risk management, and establishing common methodologies for risk assessment. In particular, it should contribute to harmonisation of appropriate technical and organisational security measures.***~~

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~~ **storing of** information, or ~~to~~ gain**ing** 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 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.

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

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 **prior** consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

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.

6a. Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive, traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the network and information security, as defined by Article 4 (c) of Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, of a public electronic communication service or network, except where such interests are overridden by the interests for the fundamental rights and freedoms of the data subject. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity.

(26a) The processing of traffic data for network and information security purposes, ensuring the availability, authenticity, integrity and confidentiality of stored or transmitted data will enable the processing of such data for the legitimate interest of the data controller for the purpose of preventing unauthorized access and malicious code distribution, stopping the denial of service attacks, and damages to computer and electronic communication systems. The European Network and Information Security Agency (ENISA) should publish regular studies with the purpose of illustrating the types of processing allowed under Article 6 of this Directive.

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 **(including short message services (SMS) and multi media services (MMS))** for the purposes of direct marketing may ~~**only**~~ be allowed **only** 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**~~ **at the time of the collection of the contact details** 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**, taking into account that both options must be free of charge for the subscriber.**

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 in contravention of Article 6 of Directive 2000/31/EC,** 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.

6. Without prejudice to any administrative remedy for which provision may be made, *inter alia* under Article 15(a)(2), Member States shall ensure that any individual or legal person ~~having a legitimate interest in combating of~~ 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 ~~or the interests of their customers~~, may take legal action against such infringements before the courts. Member States may also law down specific rules on penalties applicable to providers of electronic communications services which by their inaction contribute to infringements of national provisions adopted pursuant to this Article.

*(35) Electronic communications service providers have to make substantial investments in order to combat unsolicited commercial communications ("spam"). They are also in a better position than end-users in possessing the knowledge and resources necessary to detect and identify spammers. E-mail service providers and other service providers should therefore have the possibility to initiate legal action against spammers **for such infringements** and thus defend the interests of their customers as ~~well as~~ **part of** their own legitimate business interests.*

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.

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.

~~***Article 14a***~~

~~**Committee**~~

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

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

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

Article 15

Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1(1) of that Directive.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 15a
Implementation and enforcement

1. Member States shall lay down the rules on penalties 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 if the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by the <time-limit for implementation of the amending act> at the latest 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 ~~national regulatory~~ 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 ~~national regulatory~~ competent national authorities and, where relevant, other national bodies have all investigative powers and resources necessary, including the possibility to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4. In order to ensure effective cross-border co-operation 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 Commission may adopt ~~technical implementing measures~~ recommendations, following consultation with ~~the Authority~~ ENISA, the Article 29 Working Party and the relevant regulatory authorities.

~~The 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). On imperative grounds of urgency, the Commission may use the urgency procedure referred to in Article 14a (3).~~

(36) 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 n****ational* ~~***regulatory***~~ *authorities* ***and, where appropriate, other relevant national bodies*** *should have sufficient powers and resources to investigate cases of non-compliance effectively, including the possibility to obtain any relevant information they might need, to decide on complaints and to impose sanctions in cases of non-compliance.*

(36a) 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 those cases, procedures relating for example to the quantity and format of the information exchanged between authorities or the deadlines to be complied with should be defined in recommendations. Such procedures will also allow the resulting obligations on market actors to be harmonised, contributing to the creation of a level playing field in the Community.

(38) The measures necessary for the implementation of the Universal Service Directive ~~***and the 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.*

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 4
Transposition

Article 5
Entry into force

Article 6
Addressees]