

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12 July 2000
COM(2000) 385

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**concerning the processing of personal data and the protection of privacy in the
electronic communications sector**

(presented by the Commission)

EXPLANATORY MEMORANDUM

1. INTRODUCTION

The proposed Directive is intended to replace Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, which was adopted by the European Parliament and the Council on 15 December 1997 and had to be transposed by 24 October 1998 at the latest.

The proposal is not intended to create major changes to the substance of the existing Directive, but merely adapts and updates the existing provisions to new and foreseeable developments in electronic communications services and technologies.

The majority of provisions of the existing Directive are therefore carried over in the new proposal, subject to minor drafting changes.

2. AIMS AND OBJECTIVES

One of the regulatory principles as set out in the context of the 1999 Review of the regulatory framework for electronic communications services, is the aim to create rules which are technology neutral, this is not to impose, nor discriminate in favour of, the use of a particular type of technology, but to ensure that the same service is regulated in an equivalent manner, irrespective of the means by which it is delivered.

This also implies that consumers and users should get the same level of protection regardless of the technology by which a particular service is delivered. Maintaining a high level of data protection and privacy for citizens is one of the declared aims of the 1999 Review.

3. PROPOSED CHANGES

Definitions and terminology

In the present proposal the existing definitions of telecommunications services and networks in Directive 97/66/EC will be replaced by definitions of electronic communications services and networks to align the terminology with the proposed Directive establishing a common framework for electronic communications services and networks. The update of these definitions is necessary to ensure that all different types of transmission services for electronic communications will be covered regardless of the technology used.

Moreover, four new definitions are added of calls, communications, traffic data and location data to strengthen the common understanding of these terms and thereby improve the harmonised implementation of the relevant articles throughout the Community.

Traffic data

In the existing Directive 97/66/EC Article 6 on traffic data only refers to 'calls', which, if interpreted in the strict sense, only refers to so-called circuit switched connections (traditional voice telephony) but not to packet switched transmissions (data transmission, use of the Internet). It is not technology neutral to protect traffic data generated in the setting up of

traditional telephone calls but not similar traffic data generated in the process of transmission of communications over the Internet.

Therefore, the existing term 'to establish a call' in Article 6.1 is replaced by 'the transmission of a communication' so as to cover all traffic data in a technology neutral way.

A further change is made to Article 6.3 by creating a possibility for further processing of traffic data, not just billing data, for the purpose of value added services with the consent of the subscriber or user. With the extension of the data protection safeguards to traffic data generated by any transmission network for electronic communications, the existing possibility for further processing of traffic data, limited to billing data and only for the direct marketing of the service providers electronic communications services, has become too narrow. Today, value added services have been developed and can be offered based on particular traffic data and there is no reason to prohibit such services in cases where the subscriber has consented to the use of traffic data for the purpose of these services.

On the other hand, it is very important for subscribers to be fully informed about the type of data which are being processed and the purposes for which this is done. For this reason, an explicit obligation to inform subscribers of the personal data which are being collected, is added in Article 6.4. This empowers the subscribers to control and, where necessary, object to ongoing data processing.

Finally, it is proposed to delete the Annex to Directive 97/66/EC on traffic and billing data. With the advent of many different electronic communications services which are billed in many different ways (metered, flat fee, pre-paid), the existing Annex does not stand the test of technological neutrality. The data mentioned in the Annex were only valid for traditional tariffication methods for traditional voice telephony. For many services which exist today, the Annex includes too many data (those which are not relevant for billing) and for other services, the list missed out certain data which are relevant for other types of payment.

Location data

In today's mobile communications networks, location data giving the geographic position of mobile users or, strictly speaking, that of their terminal equipment, already exist. This information is necessary to enable the transmission of communications from and to a user without a fixed location. For cellular networks the location data may be relatively imprecise, depending on the surface of the cell within which the mobile user happens to be. For satellite communications systems, location information necessary for transmitting communications is even less precise. This type of crude location information, which is actually a by-product of the communication transmission service, is already covered by the existing Directive under traffic data.

However, a new type of service is available over cellular and satellite networks which allows the exact positioning of a mobile user's terminal equipment. Here the location data are far more precise and are specifically processed by the network for the purpose of providing value added services to users and subscribers. An example of such services are road transport telematic services providing traffic information and guidance to drivers.

Precise location data are also useful for emergency services to be able to send assistance or rescue teams to mobile users in distress who may not always be able to describe where they are exactly.

While mobile location based services must be welcomed as they can be of great use to the public, it is also necessary to ensure appropriate data protection and privacy safeguards. The capacity of processing very precise location data in mobile communications networks should not lead to a situation where mobile users are under permanent surveillance with no means to protect their privacy, other than not using mobile communications services at all.

For those location data which are not covered by Article 6 on traffic data, a new article is proposed, stipulating that such data may only be used with the consent of the subscriber, and providing subscribers and users with a simple means to temporarily deny processing of their location data in the same way as such means exist for calling line identification under Article 10.

The only exceptions to the principle of prior consent would be the use of location data by emergency services and the existing derogations for Member States for the purposes of public and national security and criminal investigations. For this purpose an override is created in Article 11 along the lines of the existing override for blocked calling line identification which can be used by emergency services. In addition, a reference to the new Article 9 is included in Article 15.1 (ex Article 14.1) to allow Member States to use location data where this is necessary for the purposes mentioned above.

Directories of subscribers

The present article on Directories of subscribers in Directive 97/66/EC assumes that the default for subscribers listing is to be in a public directory, as it has traditionally been the case for fixed voice telephony services. It was therefore necessary to create a rather detailed list of possibilities which subscribers should have in deviation from the default option (right to be omitted from the directory, right to omit part of their address, right to have no reference to their gender) to enable them to protect their privacy.

The maintenance of including subscribers to fixed voice telephony services as a default situation in the existing Directive 97/66/EC, has been defended on the grounds that public directories of subscribers are in the interest of the public and part of universal service.

However, for new electronic communications services such as GSM and e-mail, it is no longer appropriate to assume that as a default subscribers to such services are in public directories. On the contrary, most subscribers do not want to make public their mobile telephone numbers and e-mail addresses and most service providers have in practice respected the wishes of their subscribers for good commercial reasons.

It is therefore necessary to align the Article on Directories of subscribers with this changed situation, by giving subscribers the right to determine whether they are listed in a public directory and with which of their personal data. This also allows a substantial simplification of the article because as it is no longer necessary to spell out the various privacy options which the subscriber should have. Obviously, the intention of the article is not to force directory service providers to include subscriber data beyond the purpose of the directory. The subscriber cannot insist on the inclusion of data outside the range which has been determined by the directory provider.

With a view to taking into account the various usage possibilities of , in particular, electronic public directories (such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number or other criteria), it is necessary to inform the subscribers of the respective purposes and to ensure that their

consent to be included in the directory is based on full information about the ways in which their personal data can be used.

Unsolicited communications

The existing Article 12 of Directive 97/66/EC provides protection against unsolicited calls for direct marketing purposes. However, since the term ‘call’ has been interpreted in a narrow sense some of the national transposition law has only created protection against unsolicited voice telephony calls for direct marketing purposes, with the exclusion of direct marketing messages by e-mail or other new forms of communications.

To render the Article technology neutral, the term ‘call’ is replaced by the term ‘communication’.

Moreover, electronic mail for direct marketing purposes other than at the request of a subscriber (so-called ‘spam’), will be covered by the same type of protection as exists for faxes. This means that spamming will be prohibited except with respect to subscribers who have indicated that they want to receive unsolicited e-mails for direct marketing purposes.

Four Member States already have bans on unsolicited commercial e-mail and another is about to adopt one. In most of the other Member States opt-out systems exist. From an internal market perspective, this is not satisfactory. Direct marketers in opt-in countries may not target e-mail addresses within their own country but they can still continue to send unsolicited commercial e-mail to countries with an opt-out system. Moreover, since e-mail addresses very often give no indication of the country of residence of the recipients, a system of divergent regimes within the internal market is unworkable in practice. A harmonised optin approach solves this problem.

4. PRIVACY COMPLIANCE OF SOFTWARE AND HARDWARE USED FOR ELECTRONIC COMMUNICATIONS SERVICES

In the context of the 1999 Review public consultation, some commentators have raised the question of existing software and hardware which processes personal data of the users and makes them available to third parties without the knowledge or consent of these users. The Working Party of Data Protection Commissioners established under Article 29 of Directive 95/46/EC¹ on the processing of personal data, had already addressed the problem of so-called invisible and automatic processing of personal data on the Internet performed by software and hardware. In its Recommendation 1/99 of 23 February 1999, the Working Party has described the problem of privacy invading features embedded in software and hardware used for communications over the Internet. The Working Party called on software and hardware industry to develop privacy-compliant products in line with data protection rules of the general data protection Directive 95/46/EC and the telecommunications data protection Directive 97/66/EC². Since one of the objectives of the 1999 Review of the

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ L 281, 23.11.1995, p.31).

² Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p.1).

telecommunications regulatory framework is to ensure a consistent, technology neutral application of existing rules and propose amendments were technological neutrality is not guaranteed, the possibility to address the matter in the revision of Directive 97/66/EC has been examined.

Under the Directive providers of public telecommunications services and networks are under specific legal obligations to guarantee the security of their networks, to ensure the confidentiality of communications and to delete traffic data. At the same time some of the software which is necessary for new telecommunications services such as software used for sending e-mails and browsers used for surfing the Internet, does not comply with data protection rules as the Article 29 Working Party has noted. Clearly, there is no technological neutrality in a situation where the privacy of the user is protected depending on whether certain functionalities necessary for a telecommunications service are in the network or in the software.

However, the option of amending the Directive by extending its coverage from electronic communications services and networks to terminal equipment including software, is considered inappropriate. Instead, the Commission might propose measures under Article 3.3.c) of Directive 1999/5/EC on telecommunications terminal equipment³ which explicitly foresees the possibility of requiring manufacturers of terminal equipment to construct their product in such a way that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. Such measures could be proposed if privacy compliance of soft- and hardware remains unsatisfactory.

5. DESCRIPTION OF ARTICLES

Article 1 - Object and Scope

Harmonises data protection requirements in order to allow free movement of data and of electronic communications equipment and services;

Explains link with general data protection Directive and confirms the exclusion of Title V and VI matters from scope of Directive.

(Unchanged except for replacement of 'telecommunication services' by 'electronic communications services')

Article 2 - Definitions

Aligns definitions with those of new Framework Directive, adds definitions of 'call', 'communication', 'traffic data' and 'location data'.

(Updated and extended)

Article 3 - Services concerned

Limits scope to electronic communications services available to the public

Creates derogation option for analogue exchanges.

³ 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 (OJ L 91, 7.4.1999, p.10).

(Unchanged except for replacement of ‘telecommunication services’ by ‘electronic communications services’ and deletion of reference to ISDN and digital mobile networks for technological neutrality.)

Article 4 - Security

Imposes responsibility for the security of services and networks on providers and obliges them to inform subscribers in case of residual security risks.

(Unchanged except for replacement of ‘telecommunication services’ by ‘electronic communications services’)

Article 5 - Confidentiality of communications

Guarantees confidentiality of communications including the relevant traffic data and prohibits tapping or other forms of surveillance by third parties

(Unchanged except for replacement of ‘telecommunication services’ by ‘electronic communications services’ and addition of ‘traffic data’ necessary in view of the introduction of definitions for ‘communication’ and ‘traffic data’)

Article 6 - Traffic data

Prohibits the use of traffic data except for billing purposes; extends coverage to all types of transmissions of electronic communications (not just calls); introduction of possibility for further data processing for value-added services based on consent of user/subscriber;

(Updated and extended)

Article 7 - Itemised billing

Gives subscribers right to non-itemised bills; obliges Member States to ensure availability of sufficient modalities for privacy friendly communications and payments.

(Unchanged except for small drafting change adding ‘privacy enhancing’)

Article 8 - Presentation and restriction of calling and connected line identification

Provides subscribers and users with safeguards to protect their privacy in view of calling line and connected line identification services (CLI).

(Unchanged)

Article 9 - Location data

Introduces privacy safeguards for subscribers and users with regard to mobile location information services.

(New article)

Article 10 - Exceptions

Allows access to blocked CLI information for emergency services and for tracing of malicious calls; to be extended to new article on mobile location information.

(Unchanged except for inclusion of new Article 9)

Article 11 - Automatic call forwarding

Gives subscribers the right and means to undo the forwarding of calls to their line.

(Unchanged)

Article 12 - Directories of subscribers

Gives subscribers the right to determine whether and which of their personal information shall be included in a public directory and be fully informed of the purposes of the directory.

(Article simplified and deletion of possibility to charge for the right to be excluded from a directory; takes account of new electronic communications services and new types of directory services)

Article 13 - Unsolicited communications

Gives subscribers the right to refuse unsolicited communications for direct marketing purposes; Extended to cover all forms of electronic communications.

Electronic mail to be included under the opt-in system.

(Updated and extended)

Article 14 - Technical features and standardisation

Guarantees that data protection considerations may not lead to barriers to the single market for terminal equipment and software free movement and ensures that any mandatory requirements on terminal equipment and software to protect personal data and privacy may only be imposed through Community procedures

(Update of references and terminology to new Radio and telecommunications terminal equipment Directive (1999/5/EC))

Article 15 - Application of certain provisions of Directive 95/46/EC

Specifies where Member States may restrict provisions of the Directive to safeguard public security and conduct criminal investigations.

Extends provisions of General data protection Directive on legal remedies and proceedings of working party to this Directive.

(Unchanged except for inclusion of new Article 9 in scope of derogation for public security reasons, replacement of 'telecommunication services' by 'electronic communications services' and deletion of committee procedure as their only role in the context of this directive was the amendment of the Annex which has disappeared).

Article 16 - Transitional arrangements

Transitional arrangement for editions of public directories already existing before the transposition of the Directive.

(Part of previous transitional arrangements has been deleted as they are no longer relevant following transposition of Directive 97/66/EC)

Article 17 - Transposition

Provides ultimate date of transposition.

(Date adapted)

Article 18 - Entry into force

(Standard clause)

Article 19 - Addressees

(Standard clause)

Conclusion

The present proposal aims to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used.

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**concerning the processing of personal data and the protection of privacy in the
electronic communications sector**

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 Commission¹,

Having regard to the opinion of the Economic and Social Committee²,

Having regard to the opinion of the Committee of the Regions³,

Acting in accordance with the procedure laid down in Article 251 of the Treaty⁴,

Whereas:

- (1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁵ requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.
- (2) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.
- (3) Directive 97/66/EC of the European Parliament and of the Council of 15 Decemebr 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector⁶ translated the principles set out in Directive 95/46/EC in specific rules for the telecommunications sector . That Directive has to be adapted to

¹ OJ C , , p. .

² OJ C , , p. .

³ OJ C , , p. .

⁴ OJ C , , p. .

⁵ OJ L 281, 23.11.1995, p.31

⁶ OJ L 24, 30.01.1998, p.1.

developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used.

- (4) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data, The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.
- (5) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.
- (6) In the case of public communications networks, specific legal, regulatory, and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.
- (7) Legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.
- (8) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.
- (9) In the electronic communications sector, Directive 95/46/EC applies in particular for all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals applies. Directive 95/46/EC applies to non-public communications services.
- (10) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. It is for Member States to take such measures as are necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. This Directive does not affect the ability of Member

States to carry out lawful interception of electronic communications if necessary for any of these purposes.

- (11) Subscribers of a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed to protect the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. The Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.
- (12) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.
- (13) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which are outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. Security is appraised in the light of Article 17 of Directive 95/46/EC.
- (14) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.
- (15) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform for the marketing of its own electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his consent to such processing. Traffic data used for marketing of own communications services or for the provision of value added services should also be

erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

- (16) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States must encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card.
- (17) In digital mobile networks location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.
- (18) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular helplines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.
- (19) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others and, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.
- (20) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are

published in a directory and if so, which. Providers of public directories should inform the subscribers included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

- (21) Safeguards should be provided for subscribers against intrusion of their privacy by means of unsolicited calls, telefaxes, e-mails and other forms of communications for direct marketing purposes. Member States may limit such safeguards to subscribers who are natural persons.
- (22) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technology neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity⁷ will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.
- (23) In particular, similarly to what is provided for by Article 13 of Directive 95/46/EC, Member States can restrict the scope of subscribers' obligations and rights in certain circumstances, for example by ensuring that the provider of a publicly available electronic communications service may override the elimination of the presentation of calling line identification in conformity with national legislation for the purpose of prevention or detection of criminal offences or of State security.
- (24) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.
- (25) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

⁷ OJ L 91, 07.4.1999, p.10.

- (26) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope and aim

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
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 legitimate interests of subscribers who are legal persons.
3. This Directive shall not apply to activities which fall outside the scope of Community law, 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

1. Save as otherwise provided, the definitions given in Directive 95/46/EC and in Directive 2001/./EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services, shall apply for the purposes of this Directive. The following definitions shall also apply :
 - (a) ‘user’ shall mean 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’ shall mean any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network;
 - (c) ‘location data’ shall mean 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' shall mean any information exchanged or transmitted between a finite number of parties by means of a publicly available electronic communications service;
- (e) 'call' shall mean a connection established by means of a publicly available telephone service allowing two-way communication in real time.

Article 3

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.
2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.
3. Cases where it would be technically impossible or require a disproportionate investment to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data, by persons other than users, without

the consent of the users concerned, except when legally authorised to do so, in accordance with Article 15 (1).

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Article 6

Traffic data

1. Traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by the provider of a public communications network or service must be erased or made anonymous upon completion of the transmission, without prejudice to the provisions of paragraphs 2, 3 and 4.
2. Traffic data which are 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 its own electronic communications services or for the provision of value added services to the subscriber, 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, if the subscriber has given his consent.
4. The service provider must inform the subscriber of the types of traffic data which are processed for the purposes mentioned in paragraphs 2 and 3 and of the duration of such processing.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 services handling billing or traffic management, customer enquiries, fraud detection, marketing the provider's own 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 authorities to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.
2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and

called subscribers, for example by ensuring that sufficient alternative privacy enhancing modalities for 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 calling user must have 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 called subscriber must have 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 called subscriber must have 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 called subscriber must have the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.
5. The provisions of paragraph 1 shall also apply with regard to calls to third countries originating in the Community. The provisions of 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

1. Where electronic communications networks are capable of processing location data other than traffic data, relating to users or subscribers of their services, these 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 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.

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 in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the electronic 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, 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, free of charge, to determine whether their personal data are included in public directories, 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.

3. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
2. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, by means other than those referred to in paragraph 1, 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.
3. The provisions of 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 unsolicited communications are sufficiently protected.

Article 14

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.
2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and the Council of 22 June 1998 laying down a

procedure for the provision of information in the field of technical standards and regulations⁸, as amended by Directive 98/48/EC⁹

3. Where required, the Commission shall adopt measures to ensure that terminal equipment incorporates the necessary safeguards to guarantee the protection of personal data and privacy of users and subscribers, 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 telecommunications¹⁰.

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 when such restriction constitutes a necessary measure to safeguard national security, defence, public security, 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.
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 established by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of Directive 95/46/EC with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 16

Transitional arrangements

Article 12 shall not apply to editions of directories published before the national provisions adopted pursuant to this Directive enter into force.

⁸ , OJ L 204, 21.7.1998, p.37.

⁹ OJ L 217, 5.8.1998, p.18.

¹⁰ OJ L 36, 7.2.1987, p.31, Decision as last amended by the 1994 Act of Accession.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 December 2001 at the latest. They shall forthwith inform the Commission thereof.
2. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.
3. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18

Entry into force

This Directive shall enter into force on the 20th day following that of its publication in the *Official Journal of the European Communities*.

Article 19

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

FINANCIAL STATEMENT

The financial implications of this Directive are covered by the Financial Statement in the Directive on *a common regulatory framework for electronic communications networks and services*.

IMPACT ASSESSMENT FORM

THE IMPACT OF THE PROPOSAL ON BUSINESS WITH SPECIAL REFERENCE TO SMALL AND MEDIUM-SIZED ENTERPRISES(SMEs)

TITLE OF PROPOSAL

Proposal for a directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector.

THE PROPOSAL

1. *Taking account of the principle of subsidiarity, why is Community legislation necessary in this area and what are its main aims?*

The Directive is one element in a new regulatory framework which seeks to ensure that the electronic communications sector continues to develop as a competitive market delivering benefits to all companies and individuals in the Community that use electronic communications services.

The importance of consolidating the single market in this area is widely supported, and adaptation of existing Community measures is recognised as the most effective way of achieving this.

The present proposal mainly updates the existing Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector to take account of new services and technological developments. The aim is to cover all electronic communications services in a technology neutral fashion. A harmonised level of data protection in the electronic communications sector is an essential element for the functioning of the internal market in electronic communications services and networks.

THE IMPACT ON BUSINESS

2. *Who will be affected by the proposal?*

All providers of electronic networks and services and providers of directory services will be affected by the proposal. However, in most cases the present proposal will not change the legal obligations as already exist under the present Directive.

3. *What will business have to do to comply with the proposal?*

Businesses need to adopt good data protection practices, as defined by the proposal for a Directive, in the design and management of the services and networks they provide.

4. *What economic effects is the proposal likely to have?*

As explained above, most of the provisions of this proposal are already applicable under the existing Directive 97/66/EC. The economic effects at the level of individual businesses are likely to be minimal. However, the proposal is intended to stimulate general consumer

confidence in electronic communications services which is necessary for a prosperous development of these services and of electronic commerce.

5. *Does the proposal contain measures to take account of the specific situation of small and medium-sized firms (reduced or different requirements etc)?*

Articles 12 and 13 on directories and unsolicited communications require Member States to take account of the legitimate interests of subscribers to electronic communications services who are legal persons with regard to the publication of their data in public directories and with regard to possibilities to protect themselves against unsolicited communications for direct marketing purposes. These provisions recognise that small and medium sized firms may have similar problems as individuals in these two areas.

CONSULTATION

6. *List the organisations which have been consulted about the proposal and outline their main views.*

The Commission consulted on many aspects of these proposals in the 1999 Communications Review Communication in November 1999 (COM(1999)539). 229 organisations or individuals responded. A list may be found at the following web address: <http://www.ispo.cec.be/infosoc/telecompolicy/review99/comments/comments.html>. Their main views are summarised in the Communication reporting on the results of the public consultation (COM(2000)239). Furthermore, a working document summarising the key provisions of this proposal was issued on 28 April, to which 128 organisations or individuals responded. A list may be found at the following web address:

<http://www.ispo.cec.be/infosoc/telecompolicy/review99/nrfwd/comments.html>.