



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 21 June 2001

10173/01

**Interinstitutional File:
2000/0189 (COD)**

LIMITE

**ECO 188
CODEC 634**

OUTCOME OF PROCEEDINGS

from : COREPER

dated : 20 June 2001

to : COUNCIL

No. Cion prop. : 10961/00 ECO 242 CODEC 616

N° prev. doc. 9337/01 ECO 146 CODEC 491

Subject : 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

At its meeting of 20 June 2001, the Permanent Representatives Committee finalised the draft text of the above proposal for a Directive which is attached in the Annex and agreed to submit it to the Council. This text is to be read in conjunction with the report to Council set out in doc. 10200/01 ECO 191 CODEC 639 where the outstanding issues and the remaining reservations are presented.

Draft**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
concerning the processing of personal data and the protection of privacy in the electronic
communications sector¹***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 the EC Treaty, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

*Article 2²**Definitions*

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2001/.../EC of the European Parliament and of the Council of ... [on a common regulatory framework for electronic communications networks and services], 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;

¹ The recitals will be finalised at a later stage.

² New Recital: "The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided; Prepaid cards are also considered as a contract."

- (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;³
- (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;⁴
- (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;⁵

³ New Recitals: "A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may inter alia consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection; they may also consist of the format in which the communication is conveyed by the network."

"The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection, for electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider."

⁴ Addition to the above recital on traffic data: " Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time, to the time the location information was recorded."

⁵ New Recital: "Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive."

Minutes statement: "The German delegation notes with reference to Art. 2 d) and the corresponding recitals of the 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, that in Germany the pure content services are subject to specific data protection laws, that are not affected by this directive."

- (e) 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time.
- (f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC.⁶
- (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.⁷
- (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.

Article 3

Services concerned

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

⁶ New Recital: "For the purposes of this Directive consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and otherwise determined within Directive 95/46/EC."

⁷ Addition to Recital (15): "value added services may for instance consist of advise on least expensive tariff packages, route guidance , traffic information, weather forecasts, tourist information".

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 electronic 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 is 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.⁸

⁸ Addition to Recital (13): "The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at his own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message".

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.⁹
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.¹⁰

⁹ New Recital: "The prohibition of storage of communications by others than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent that such information may be further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased."

¹⁰ New Recital: "Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should to be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged."

Article 6

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or 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 the provisions of paragraphs 2, 3, 5 and Article 15, paragraph 1.¹¹
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.¹²
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 consent.¹³

¹¹ New Recitals

"The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the Domain Name System of IP-addresses or the caching of IP-address to physical address bindings or the use of log in information to control the right of access to networks or services."

"The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service indicated by concrete facts."

¹² New Recital: "Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data they should be considered as value added services for which the consent of the subscriber is required."

¹³ New Recital: "Whether the consent to be obtained for the processing of personal data in view of providing a particular value added service must be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it."

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 in paragraph 3.
5. Processing of traffic data, in accordance with paragraphs 1 to 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 electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.
6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.
2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing 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 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. 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 to 4.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of electronic communications networks or services can be processed, 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 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 electronic communications network or 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.¹⁴

¹⁴ New Recitals:

" Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, this subcontracting and subsequent data processing must be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC."

"Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data."

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 12¹⁵

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge, about the purpose(s) of printed or electronic directories 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.
 - 2a. Member States shall ensure that for any purpose of a public directory other than the search of communication details of persons on the basis of their name and, where necessary, a minimum of other identifiers, the additional consent of the subscribers is required.
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.

¹⁵

New Recital:

"The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber must be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted"

Article 13

Unsolicited communications¹⁶

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. 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.

¹⁶

Addition to Recital (21) :

"These provisions cover unsolicited communications inter alia in political campaigns and charity fund raising."

New Recital:

"This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) are fully applicable."

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.
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.

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) to (4), and Article 9 of this Directive 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. To this end Member States may inter alia provide for the retention of data for a limited period justified on the grounds laid down in this paragraph, in accordance with the general principles of Community law.
2. The provisions of Chapter III on Judicial Remedies, Liability and Sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.
3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 16

Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.
2. Where the personal data of subscribers to fixed public voice telephony services have been included in a public subscriber directory in conformity with the provisions 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, unless subscribers indicate otherwise, after having received complete information about purposes and options in conformity with Article 12 of this Directive.
3. Where companies have obtained communication details for electronic mail, such as addresses or numbers, from customers in the context of the purchase of a product or service, in accordance with Directive 95/46/EC, before the national provisions adopted in pursuance of this Directive enter into force, these communication details may continue to be used for direct marketing of other products or services by the same company, provided that customers are given the opportunity to stop free of charge such use of their communication details at the occasion of each message.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 15 month after the date of its entry into force at the latest. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.
2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18

Entry into force

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

Article 19

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament

For the Council

The President The President
