TRANSLATION OF LETTER

from: Commission of the European Communities, signed by Mr Jean DONDELINGER, Member
dated: 27 July 1990
to: Mr Gianni DEMICHELIS, President of the Council of the European Communities
Subject: Protection of individuals in relation to the processing of personal data in the Community and information security

Sir,

I enclose a Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security, accompanied by the following documents:

(a) a proposal for a Council Directive on the approximation of certain laws, regulations and administrative provisions of the Member States on the protection of individuals in relation to the processing of personal data
(b) a draft Resolution of the Representatives of the Governments of the Member States meeting within the Council on the application of the principles of the Directive to those parts of the public sector which do not fall within the scope of Community law
(c) a Commission declaration on the application to the institutions and other bodies of the European Communities of the principles contained in the Council Directive on the approximation of certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data
(d) a proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks SYN 288

(e) a Recommendation for a Council Decision on the opening of negotiations with a view to the accession of the European Communities to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data

(f) a proposal for a Council Decision in the field of information security.

Community action in the field of the protection of individuals in relation to the processing of personal data is necessary for the completion of the internal market and to ensure the development of the data processing industry and of new telecommunications services.

Accordingly, besides a framework Directive which is the central feature of the protection system in the internal market and which is accompanied by measures extending the same principles of protection to the Community bodies and to activities not falling within the scope of Community law, the Commission is proposing sectoral measures specific to telecommunications.

Since the proposals at (a) and (d) are based on Article 100a of the Treaty establishing the European Economic Community, the procedure for co-operation with the European Parliament and consultation of the Economic and Social Committee are mandatory.

Since the proposal at (f) is based on Article 235 of the Treaty establishing the European Economic Community, consultation of the European Parliament is mandatory. In view of the subject-matter, the Commission suggests that the Economic and Social Committee also be consulted.

The Council should adopt its common position on the proposals at (a) and (d) and act on the proposal at (f) in March 1991. With this in mind, the European Parliament and the Economic and Social Committee should deliver their Opinions before the end of the year.

(Complimentary close).

(s.) Jean DONDELINGER
COMMISSION OF THE EUROPEAN COMMUNITIES

COM(90) 314 final - SYN 287 and 288
Brussels, 13 September 1990

COMMISION COMMUNICATION
on the protection of individuals in relation to the processing of
personal data in the Community and information security

Proposal for a
COUNCIL DIRECTIVE
SYN 287
concerning the protection of individuals
in relation to the processing of personal data

Draft
RESOLUTION OF THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER
STATES OF THE EUROPEAN COMMUNITIES MEETING WITHIN THE COUNCIL

COMMISSION DECLARATION
on the application to the institutions and other bodies of the European
Communities of the principles contained in the Council
Directive
concerning the protection of
individuals in relation to the processing of personal data

Proposal for a
COUNCIL DIRECTIVE
SYN 288
concerning the protection of personal data and privacy in the context
of public digital telecommunications networks, in particular the integrated
services digital network (ISDN) and public digital mobile networks

Recommendation for a
COUNCIL DECISION
on the opening of negotiations with a view to the accession of the
European Communities to the Council of Europe Convention for the protection
of individuals with regard to the automatic processing of personal data

Proposal for a
COUNCIL DECISION
in the field of information security
1. INTRODUCTION

1. The increasingly frequent recourse to the processing of personal data in every sphere of economic and social activity and the new data-exchange requirements linked to the strengthening of European integration necessitate the introduction in the Community of measures to ensure the protection of individuals in relation to the processing of personal data and to enhance the security of information processing in the context, notably, of the development of open telecommunications networks.

2. At a time when progress in the field of information technology is making it much easier to process and exchange all sorts of data, the current position with regard to the protection of individuals in relation to such processing in the Community is characterized by the diversity of national approaches. In the 1970s, the concern felt about the protection of individuals in relation to the processing of personal data led to the legislative process being set in motion in several Member States with a view to limiting and providing a framework for the use of this kind of data. At the last count, however, only seven Member States had specific laws in this field. Moreover, although their objectives are the same,
those laws sometimes adopt divergent approaches, for example on the question of scope (inclusion or not of manual data files, protection or not of legal persons) or on the question of the preconditions for processing (extent of the obligation to notify, provision of information at the time of collection, processing of sensitive data).

3. Over and above national provisions and in addition to the recommendation of the Council of the OECD concerning guidelines on the protection of privacy and the cross-border flow of personal data of 23 September 1980, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data is the only international legal instrument in this field. However, it leaves open a large number of options for the implementation of the basic principles it contains, and it has been ratified by only seven Member States, of which one still has no domestic legislation.

4. This state of affairs has given cause for concern for some time in the Community. In a number of resolutions dating back to 1976, the European Parliament has voiced its disquiet and called upon the Commission to prepare a proposal for a directive harmonizing laws on the protection of personal data.

5. The Commission, in a recommendation of 29 July 1981, stated that such protection is quite fundamental and that it is desirable that there should be an approximated level of protection in all the Member States. It recommended the Member States to ratify, before the end of 1982, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. It added, however, that "If all the Member States do not within a reasonable time sign and ratify the Convention, the Commission reserves the right to propose that the Council adopt an Instrument on the basis of the EEC Treaty".

---

1 OJ No C 100, 3.5.1976, p. 27; OJ No C 140, 5.6.1979, p. 34; OJ No C 87, 5.4.1982, p. 39.
6. The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded just when it is becoming essential to the activities of business enterprises and research bodies and to collaboration between Member States' authorities in the frontier-free area provided for in Article 8a of the Treaty. With this in mind, the Strasbourg European Council of 8 and 9 December 1989 stressed, in the context of measures to promote the free movement of persons and People's Europe, the need "to ensure that the procedures for cooperation between administrations first ensure the protection of individuals with regard to the use of personalized data banks".

7. A Community approach towards the protection of individuals in relation to the processing of personal data is also essential to the development of the data processing industry and of value-added data communication services. The speedy introduction of harmonized provisions concerning the protection of data and privacy in the context of digital telecommunications networks is a key element in the completion of the internal market in telecommunications equipment and services.

8. The penetration of data processing into every sphere of economic and social activity and the appearance of global communication systems making it easier to integrate various activities also represent a new challenge which calls for the affording of "protection" commensurate with the risks involved in any technical or human failure, whether it be accidental or deliberate. Effective information security is indispensible if one is to ensure effective protection of privacy and preserve the integrity of the present wealth of data recorded and transmitted electronically. The Community policies and programmes for the development of the data processing and telecommunications industries and the completion of the internal market might be seriously undermined if an active policy for the creation, development and promotion of information security standards is not adopted. Since telecommunications nowadays make it possible to exchange data worldwide, such a policy must take that dimension into account. It is, moreover, essential that national information security policies do not become an obstacle to the promotion of the harmonious development of the Community and to relations with third countries.
II. THE PROPOSED APPROACH

9. The proposed approach is designed to ensure a high level of protection via a Community system of protection based on a set of complementary measures.

A. A high level of protection

10. Since the object of national laws in this field is to protect the fundamental rights of individuals, and in particular the right to privacy, and since the Community has itself stressed the importance it attaches to fundamental rights, in particular in the third paragraph of the Preamble to the Single European Act, the action taken by the Community must not have the effect of reducing the level of protection but, on the contrary, of ensuring a high level of protection throughout the Community. Through Community action it is possible to guarantee a high level of equivalent protection in all the Member States of the Community, and in so doing remove obstacles to the establishment of the Internal market in accordance with Article 100a.

11. In addition to the approximation, at a high level, of the rights of individuals, the launching of an active policy on information security is essential. Information security is vital not only to individuals but also to trade, Industry and public authorities. The important thing is to ensure effective and practical security of information held in electronic form while avoiding the formation of new technical obstacles between Member States or vis-à-vis third countries. This requirement calls for the examination at Community level of the possible needs and options in close collaboration with Industry and the Member States.

B. A global approach

12. In order to establish in the Community a system of protection of individuals in relation to the processing of personal data, several measures covering the various aspects of the matter must be adopted.
13. At the internal level, besides a framework directive approximating certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data (general directive), which is the centrepiece of the protection system, a set of other, complementary measures is proposed in order to ensure the fullest possible protection. Each of the measures proposed is tailored to a specific situation, but all take as point of departure the same protection principles to be found in the general directive. A resolution of the representatives of the Governments of the Member States meeting within the Council and a Commission declaration are thus designed to make the principles contained in the directive applicable to data files which are not covered by it. Similarly, a sectoral directive is necessary in the context of public digital telecommunications networks. Lastly, information security calls for a Community action plan.

14. At the external level, the European Community must promote among its partners the introduction of adequate protection measures and support the efforts of the Council of Europe in this field. It is desirable in this connection that the Community should enter into negotiations with a view to its accession to Council of Europe Convention No 108.

This set of proposals cannot be split up without detracting from the homogeneity and cohesion of the protection system proposed.

C. Outline of the proposals

15. The proposal for a general directive is aimed at establishing an equivalent, high level of protection in all the Member States of the Community in order to remove the obstacles to the exchange of data which is necessary if the internal market is to function. To that end, the principles set forth in the draft proposal for a directive must be underwritten by the Member States. Those principles relate to the conditions under which the processing of personal data is lawful, the
rights of the data subject (right to information, right of access, right to rectification, right of opposition, etc.), the requisite data quality (data must be accurate, collected fairly, stored for specified and lawful purposes, etc.) and the setting-up of a Working Party on the Protection of Personal Data to advise the Commission on data protection issues. The draft proposal for a directive covers both the private sector and those activities of the public sector which fall within the scope of Community law. Since every individual will enjoy in each Member State an equivalent, high level of protection in respect of the processing of personal data, the Member States will no longer be able to restrict the flow of such data in the Community on grounds of the protection of the data subject.

16. The draft resolution of the representatives of the Member States of the European Communities meeting within the Council is designed to extend the coverage of the principles contained in the general directive to include files held by those parts of the public sector to which it does not apply, that is to say those authorities whose activities are not governed by Community law. For the sake of consistency, all files held by public authorities, even those which are not covered by the general directive, should be subject to the same protection principles. To that end, the Member States should commit themselves to setting in motion the necessary domestic legislative procedures.

17. The Commission declaration on the application to the institutions and other bodies of the Community of the provisions of the general directive is an expression of the Commission's wish that the principles contained in the directive should apply to the institutions and other bodies of the Community. It provides in this respect that the Commission will take and propose the necessary measures, and indicates that, in the mean time, it will apply the directive's provisions to its own data files.
18. The proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated services digital network (ISDN) and public digital mobile networks supplements the general directive by applying the general principles of data protection to the specific requirements of the new telecommunications networks. The directive seeks to guarantee telecommunications users in all the Member States a basic level of protection via measures which must be integrated into the services provided by the new networks. The Council and the European Parliament have stressed on a number of occasions the importance of appropriate measures to ensure the protection of data and privacy in the light of future developments in telecommunications, and in particular the ISDN.1 This concern was expressed strongly by the Member States' officials in charge of data protection at their annual meeting in Berlin in August 1989.

19. The recommendation for a Council Decision on the accession of the European Community to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is one of the external aspects of the Community's approach to the protection of personal data. Accession to the Convention will ensure, in relations between the Community and the third countries which will be parties thereto, the protection of data subjects and the cross-border flow of personal data.

20. The proposal for a Council Decision on the adoption of a two-year action plan on Information security completes the set of measures for strengthening the rights of individuals in relation to the processing of personal data. Information security, that is to say the protection of data stored, processed and transmitted electronically against every kind of threat (both accidental and deliberate) is essential if the rights of individuals in relation to the processing of personal data are to be effectively exercised. More generally, it is a primary requirement from

---

the point of view of the protection of property and persons which, in the
countext of the deployment of open telecommunications networks, necessitates
the development of a global strategy, concerted action at Community level
on technologies, standards and approval and testing procedures, and
technological developments involving cooperation at the pre-competitive
research and development stage.

21. The proposed action plan provides for the development of a strategic
framework for information security, the analysis of security requirements,
the devising of ways of satisfying certain priority needs, the drawing-up
of specifications, standards and validation tests, the integration of
technological and operational developments in the field of information
security into a general strategic framework and the integration of certain
security functions into information systems.
PROPOSAL FOR A
COUNCIL DIRECTIVE

CONCERNING THE PROTECTION OF INDIVIDUALS
IN RELATION TO THE PROCESSING OF PERSONAL DATA
I. Introduction

II. The need for protection in the Community
   - The diversity of national laws and the lack of an equivalent level of protection
   - Consequences for the Community

III. The approach adopted
   - An equivalent level of protection in the Community
   - A high level of protection

IV. Discussion of the provisions

This proposal for a directive is aimed at establishing an equivalent, high level of protection in all the Member States of the Community in order to remove the obstacles to the data exchanges that are necessary if the internal market is to function. To that end, the principles set forth in the draft proposal for a directive must be underwritten by the Member States. Those principles relate to the conditions under which the processing of personal data is lawful, the rights of the data subject (right to information, right of access, right to rectification, right of opposition, etc.), the requisite data quality (data must be accurate, collected fairly, stored for specified and lawful purposes, etc.) and the setting-up of a Working Party on the Protection of Personal Data to advise the Commission on data protection issues. The draft proposal for a directive covers both the private sector and those activities of the public sector which fall within the scope of Community law. Since every individual will enjoy in each Member State an equivalent, high level of protection in respect of the processing of personal data, the Member States will no longer be able to restrict the flow of such data in the Community on grounds of the protection of the data subject.
Explanatory memorandum

I. INTRODUCTION

The concern that has been felt for the past fifteen years or so about the protection of individuals in relation to the processing of personal data has arisen as a result both of the opportunities afforded by technical progress in the information processing field and of the increasingly frequent recourse that is being had to personal data processing in a multitude of spheres. This concern has manifested itself in a variety of ways and has led to the legislative process being set in motion in several Member States. On the wider international canvas, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data is as yet the only international legal instrument in this field. The OECD has laid down guidelines on the protection of privacy and transborder flows of personal data in a Recommendation of 23 September 1980, and the UN is in the process of drawing up its own guidelines.

Similar expressions of concern have been voiced in the Community context. The European Parliament has since 1976 adopted a number of resolutions in which it makes clear its disquiet on this issue and calls upon the Commission to prepare a proposal for a directive harmonizing personal data protection laws. (1)

The Commission, in a recommendation of 29 July 1981, stated that such protection is quite fundamental and that it is desirable that there should be an approximated level of protection in all the Member States. It

(1) OJ No C 100, 3.5.1976, p. 27; OJ No C 140, 5.6.1979, p. 34; OJ No C 87, 5.4.1982, p. 39.
recommended the Member States to ratify the Council of Europe Convention before the end of 1982, adding, however, that "if all the Member States do not within a reasonable time sign and ratify the Convention, the Commission reserves the right to propose that the Council adopt an instrument on the basis of the EEC Treaty".

The Strasbourg European Council of 8 and 9 December 1989 emphasized, in the context of measures to promote the free movement of persons and People's Europe, the need "to ensure that the procedures for cooperation between administrations first ensure the protection of individuals with regard to the use of personalized data banks".

In addition to these pronouncements on the need for general protection, the feelings of concern have also been translated into specific or sectoral Community measures, especially in the field of the new Information technologies.

In view of the current situation with regard to the processing of personal data and the requirements of European integration, a directive aimed at protecting individuals in connection with this type of processing is now essential.

II. THE NEED FOR PROTECTION IN THE COMMUNITY

The diversity of national laws and the lack of an equivalent level of protection in the Community

A wide variety of approaches are taken in the Member States towards the protection of individuals in relation to personal data: some Member States have no specific laws in this field, and where they do, the content differs.

Currently, seven Member States have specific laws (Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom). Work is in progress in certain other Member States.
While the object of these national laws is the same, namely to protect the data subject, they adopt different approaches owing to the multiplicity of possible ways of affording such protection. The covering of manual data files, the protection of legal persons, the procedures prior to the creation of files, the extent of the obligation to notify, the provision of information at the time of collection of data, the processing of sensitive data and transfer to other countries are just some of the questions which can be approached in different ways. Moreover, technical developments may induce countries to react differently and, in so doing, increase the diversity.

The abovementioned Council of Europe Convention has not led to a reduction in this diversity because, firstly, it leaves open a large number of options as far as implementation of its basic principles is concerned, and secondly, it has been ratified by only seven Member States (Denmark, France, Germany, Ireland, Luxembourg, Spain and the United Kingdom), of which one (Spain) still has no domestic legislation. The Commission recommendation of 29 July 1981 calling on the Member States of the Community to ratify the Convention has not altered matters.

Owing to the diversity of national approaches, the protection of individuals in relation to the processing of personal data is not equivalent in all the Member States, the level of protection varying from one Member State to another.

**Consequences for the Community**

In the Community, this state of affairs gives rise to three types of difficulty:

- The lack of specific national laws or their deficiencies do not reflect the Community's commitment to the protection of fundamental rights, as stressed in the joint declaration of the European Parliament, the Council and the Commission on fundamental rights of 5 April 1977 and in the third paragraph of the preamble to the Single European Act. What is more, in Community law, the protection of fundamental rights forms an integral part of the general principles of law which the Court of Justice of the European Communities is charged to uphold.
Where it respects the rights of the data subject, the flow of personal data is a necessity as far as the establishment and functioning of the internal market are concerned. In view of technical developments in information processing, notably the introduction of digital telecommunications networks in the Community, the cross-border dimension of data flows is apparent at three levels:

1. Personal data are used at numerous stages of economic activity. The free movement of goods, persons, services and capital requires that personal data be transferable between business people involved in cross-border activities.

2. In the Community integration process, and in particular in the context of the abolition of frontiers, cooperation between national authorities will necessarily increase, the authorities in one Member State being called upon to perform tasks which are normally the responsibility of an authority in another Member State. The flow of data is essential to such cooperation. The duty to collaborate or provide information, which will be imposed on authorities by Community law, requires at the same time that data subjects be fully protected.

3. Data exchanges are also necessary for scientific cooperation purposes.

This need to permit data flows between Member States currently comes up against the differences in national approaches to the question of protecting individuals in relation to the processing of personal data. These differences may induce a Member State to place barriers in the way of the free flow of data on grounds of the lack or inadequacy of protection in the country of origin or destination.

These differences could also, in certain circumstances, distort competition between private operators depending on the constraints to which they are subject in their country.

III. THE APPROACH ADOPTED

An equivalent level of protection in the Community

In order to afford any individual residing in the Community protection in connection with the processing of personal data and permit the flow of this
type of data between Member States, an equivalent level of protection must be established throughout the Community. To that end an approximation of laws is necessary. The Commission's programme for 1990 mentions the protection of data as a priority area in the context of completing the internal market. (1)

In this connection, Article 100a of the Treaty provides the appropriate legal basis inasmuch as a high level of equivalent protection is essential to the creation of the internal market. The completion and functioning of the internal market, which is described in Article 8a as "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of this Treaty", necessitate, for the reasons already given, an approximation of laws in this field.

In the preparation of this proposal the Commission has taken into account the requirements of Article 8c of the EEC Treaty and has concluded that no special provisions or derogations seem warranted or justified at this stage. Likewise the Commission has studied the question of the high level of health/safety/environmental and consumer protection required by the terms of Article 100a(3) of the EEC Treaty.

A high level of protection

The object of national laws in this field being to protect fundamental rights, and in particular the right to privacy, an approximation of those laws must seek to guarantee a high level of protection. Apart from the adjustments inherent in any approximation of laws, the exercise must not have the effect of reducing the level of protection already afforded in the Member States.

The general principles set out in the Council of Europe Convention are a suitable benchmark as they already constitute a common basis for the countries which have ratified the Convention. Thus, while adopting solutions compatible with those of the Convention, the Directive adds to those general principles in order to provide a high level of equivalent protection.

(1) Bull. EC Supplement 1/90, pp. 18, 25 and 27.
A high level of protection requires that the protection guaranteed by the Directive should have a very wide scope and that every situation in which the processing of personal data involves a risk to the data subject should be covered. The Directive therefore applies to manual as well as automated files and to both public-sector and private-sector files.

The principles contained in the Directive, notably those relating to the lawfulness of processing, the communication of data to third parties, notification procedures, the rights of the data subject and data quality, are designed to ensure a high level of protection by taking as a basis the various solutions adopted in national laws. Similarly, particular attention has been paid to the means of ensuring, beyond the usual arrangements for monitoring the application of Community law, the effective application of the Directive's provisions. Hence the inclusion of provisions on liability and on the setting-up of a Working Party on the Protection of Personal Data.

The principles contained in the Directive may, if necessary, be supplemented. The Directive provides in a number of its articles that Member States may lay down more specific rules in respect of data files that are subject to their law. Additional measures may also be necessary for the purpose of applying certain general principles to sectors having special features.

IV. DISCUSSION OF THE PROVISIONS

CHAPTER 1

General provisions

Article 1

Object of the Directive

This article provides that the Member States are obliged to ensure the protection of individuals in relation to the processing of personal data by
applying the Directive’s provisions. Since, under the Directive, protection is ensured in accordance with the same principles in all the Member States and is therefore equivalent, the Member States can no longer restrict, in the fields covered by the Directive, the flow of data on grounds of the protection of the data subject. The protection of individuals and the flow of data are, however, guaranteed under the Directive only in the fields covered by it. Files held for private purposes or by non-profit-making bodies cannot, therefore, give rise to the application of this article inasmuch as Article 3(2) excludes them from the scope of the Directive.

Article 2

Definitions

This article defines the main concepts used in the Directive. The definitions are taken from Council of Europe Convention N° 108 with such adjustments and clarifications as are necessary to guarantee a high level of equivalent protection in the Community.

a) "Personal data". As in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual. Depending on the use to which it is put, any item of data relating to an individual, harmless though it may seem, may be sensitive (e.g. a mere postal address). In order to avoid a situation in which means of indirect identification make it possible to circumvent this definition, it is stated that an identifiable individual is an individual who can be identified by reference to a number or a similar identifying particular.

b) "Depersonalize". This concept is designed to permit the exclusion from the scope of certain provisions of the Directive of data which are no longer identifiable. An item of data can be regarded as depersonalized even if it could theoretically be repersonalized with the help of disproportionate technical and financial resources.

c) "Personal data file". The definition is based on the criterion of possibility of access to personal data, either by means of manual processing where the file consists of a collection of structured data, or by means of automatic processing which permits the grouping together of disseminated data or the extraction of data from a complete text.
using a method of consultation which corresponds to that of a file. The definition therefore covers structured automated and manual files. Individual files, and in particular administrative files, which do not contain a structured collection of personal data are not covered owing to the specific and divergent laws governing them in the Member States.

d) "Processing". In listing the principal processing operations, the definition adapts that given in the Convention to suit the wider scope of the concept of file. Data combination operations are covered as they make it possible to produce new data (e.g. electronic profiles). The reference to blocking relates to data to which access is blocked using more stringent security measures than is normally the case, but stopping short of erasure.

e) "Controller of the file". The concept of "controller of the file" as used in the Convention is adapted in two respects: firstly, by referring to Community law in order to cover the case where specific directives contain substantive provisions on the protection of personal data; and secondly, by specifying that the person who authorizes consultation, notably in the event of direct interrogation, is the controller of the file.

f) "Supervisory authority". The definition stresses that the authority must be independent and refers to Article 26, which specifies the functions of the supervisory authority.

and h) "Public sector" and "private sector". The definitions of public sector and private sector are justified in the Directive as some of its provisions are specific to one or other sector (Chapters II and III relating to the lawfulness of personal data processing in the public and private sectors). These definitions are based on the nature of the service provided by the body concerned, regardless of its private or public status. The body will have to apply the rules specific to the private sector or to the public sector according as to whether it carries on commercial activities or performs public-service duties.
Article 3

Scope

The Directive applies to all files whose controllers are in the private sector or the public sector. In the latter case, the performance of numerous administrative tasks necessitates, by virtue of Community law, cooperation between authorities in the Member States. The Directive does not apply, however, to files in the public sector where the activities of that sector fall outside the scope of Community law (e.g. the Intelligence services).

Paragraph 2 provides for two exceptions where invasions of privacy are unlikely to occur either because the data are used for private purposes only, as is the case with a personal electronic diary, or because the files are registers of members of an association whose consent to appear therein can be presumed from their very membership and the information contained in the register is not transmitted to third parties.

Article 4

Law applicable

This article specifies the connecting factors which determine the application in each Member State of the Directive's provisions. The choice of factors in paragraph 1 is motivated by the desire to avoid a situation in which the data subject is completely unprotected owing, mainly, to the law being circumvented. The factual criterion of the place in which the file is located has therefore been adopted. In this connection, each part of a file which is geographically dispersed or divided among several Member States must be treated as a separate file.

The desire to protect the data subject in the event of relocation is at the root of a provision which requires a user consulting a file located in a third country from a terminal located in a Member State to comply with the
Directive's provisions on the lawfulness of processing, the informing of the data subject in the event of the communication of data, sensitive data, data security and liability. This requirement is imposed where such use is not simply sporadic.

In view of the ease with which files can be moved, the temporary removal of a file from one location to another does not constitute a change of location. The removal of data storage media must not give rise to the completion of formalities over and above those which have been gone through in the country in which the file is normally located.

This article is also designed to avoid any overlapping of applicable laws.

CHAPTER II

Lawfulness of processing in the public sector

Personal data may be processed only if their processing is lawful. This chapter, like Chapter III, specifies the circumstances in which processing is lawful. The lawfulness may stem from the consent of the data subject, from a provision of the Directive or of Community law, or from a national legal instrument.

Article 5

Principles

This article provides that the creation of a public-sector file and any other processing of data shall be lawful only if it is necessary for the performance of the tasks of the public authority in control of the file.

There are four cases in which data may be processed for a purpose other than that for which the file was created: if the data subject consents; if the processing has a legal basis; if, after weighing the interests involved, it is clear that the legitimate interests of the data subject do not preclude such change of purpose; and, lastly, in the event of an imminent threat to public order or a serious infringement of the rights of others.
These principles do not concern the specific case of the communication of data to third parties, which is dealt with in Article 6.

**Article 6**

Processing in the public sector having as its object the communication of personal data.

A specific provision on the communication of data to third parties is necessary inasmuch as this type of processing involves the greatest risk to the data subject. The paragraph provides for two cases in which data may be communicated to third parties, according to whether the recipient is in the public sector or the private sector. In the former instance, communication must be necessary for the performance of the tasks of the authority requesting or communicating the data; in the latter, a balancing of interests must be carried out in order to determine whether the requester has a legitimate interest and whether the interests of the data subject do not prevail.

The Member States are given the opportunity to specify in their law, within the limits of the two principles set out above, the conditions under which the communication of data is lawful. This may consist, for example, in defining, in respect of certain fields, in what circumstances the interests of the data subject prevail.

In order to ensure that the interests of the data subject are not harmed by the communication of data to the private sector, a procedure for informing the data subject is laid down. A derogation from this obligation is possible, however, where communication is authorized by the supervisory authority. The latter may attach conditions to the derogation or decide to inform the data subject itself.

**Article 7**

Obligation to notify the supervisory authority

The obligation provided for in this article to notify the supervisory authority and to have such notification recorded in a register kept by that
authority is restricted to public-sector files the data in which might be communicated. The aim is to ensure the minimum transparency necessary for the exercise of the rights of the data subject while reducing the number of formalities, as these might place a very heavy burden on the supervisory authority owing to the widely drawn concept of data file. The Member States may, however, extend the obligation to notify so as to cover other public-sector files.

CHAPTER III

Lawfulness of processing in the private sector

Article 8

Principles

The lawfulness of the processing of personal data in the private sector may be based on the consent of the data subject. Such consent must satisfy the conditions of Articles 12 (informed consent) and 13 (provision of information at the time of collection of data).

In the absence of the consent of the data subject, the lawfulness of the processing may be based on the existence of a contractual or quasi-contractual relationship between the controller of the file and the data subject in so far as the processing is necessary for the performance of the contract (e.g., processing of orders or invoicing).

The lawfulness of the processing may also be based on the fact that the data come from sources generally accessible to the public (public telephone directories) in so far as the processing is intended solely for correspondence purposes.

Lastly, the lawfulness of the processing may be based on a balancing of interests which reveals that the controller of the file has a legitimate interest and that the data subject does not have an overriding interest.

The communication of data is lawful only if it is compatible with the purpose of the file as notified (Article 11(2)), which has to be adhered to
when data are stored (Article 16(1) (b)). When data are communicated, the controller of the file is obliged, moreover, to inform the data subject in the manner prescribed in Articles 9 and 10. Within the limits of the principles set out above, the Member States may specify in their law the conditions under which the processing of data is lawful. This may consist, for example, in defining, in respect of certain fields, in what circumstances the interests of the data subject prevail.

Article 9

Obligation to inform the data subject

In order that the data subject might exercise his rights, paragraph 1 requires the controller of the file to inform the data subject of the communication of data concerning him. The data subject can thus exercise his right of access and object to continuation of the processing in question. There is no obligation to inform the data subject where the data come from sources generally accessible to the public and their processing is intended solely for correspondence purposes.

Article 10

Special exceptions to the obligation to inform the data subject

This article authorizes Member States to provide in their law that, where major practical difficulties, overriding legitimate interests of the controller of the file or a similar interest of a third party stand in the way of informing the data subject, the supervisory authority may, within the limits of the law authorizing it to do so, at the request of the controller of the file authorize a derogation from the obligation to inform the data subject. The supervisory authority may, specify the terms of the derogation and decide to inform the data subject itself. The case of major practical difficulties covers, for example, data relating to persons whose home address is not known.
Article 11

Obligation to notify the supervisory authority

For the same reasons as those underlying the obligation to notify in the public sector (Article 7), the obligation to notify in the private sector does not apply to files in which the data are not intended to be communicated or which come from sources generally accessible to the public. The notification must be updated if there is any change in the purpose of the file.

The information notified must include that which is necessary for the purpose of monitoring compliance with the Directive (at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the security measures taken). The Member States may extend the scope of the obligation to notify.

CHAPTER IV

Rights of data subjects

Article 12

Informed consent

This provision determines under what conditions the data subject's consent to the processing of data relating to him, both in the public and in the private sector, is legally valid.

The data subject's consent to the processing of data relating to him is an important justification for the processing of personal data by the controller of the file. The concept of "consent" as used in Article 12 means "informed consent". In order to enable the data subject to weigh the risks and advantages of the intended processing of data relating to him and
to exercise his rights under Article 14 of the Directive (rectification, erasure, blocking), the controller of the file has to provide the data subject with such information as is relevant to the data subject's decision, e.g. name and address of the controller of the file, purpose of the file, data stored in the file, etc.

As to the form of the consent, the Directive does not, for practical reasons, require that the data subject should give his consent in writing. The agreement, however, has to be expressly given. The consent of the data subject has to be specific in that it has to refer to the processing of data relating to him by a particular controller of a file and for a certain purpose or purposes. The agreement must also indicate the kinds of data which may be processed, the forms of processing and the potential recipients in case of transfer to third parties.

Under Article 12(c) the data subject is entitled to withdraw his consent at any time. The revocation, however, bears no retroactive effect as otherwise a previously lawful processing of personal data would be made illegal ex post facto.

Article 13

Provision of Information to the data subject at the time of collection of data

Effective data protection requires that the data subject be kept fully informed about the processing of personal data relating to him, not only once they are stored and processed in a data file but at the stage preceding their processing, i.e. at the stage of their collection.

It is laid down in Article 16(1)(a) that data must be collected fairly and lawfully. For the purposes of Article 13 this requirement covers the situation where data are obtained from the data subject himself.

The fair and lawful collection of personal data presupposes that the data subject makes his decision whether or not to disclose data relating to him
to the collectors on a reliable factual basis as regards the purpose of the processing, the identity of the controller of the file and the question whether he is under a legal obligation to disclose the data or whether disclosure is voluntary. So that he can assert his rights under Article 14 of the Directive and control effectively the use of data relating to him, he should also be informed about his rights of access and rectification and about recipients of the data.

Article 13(1) of the Directive obliges the Member States to provide in their domestic data protection laws that the data subject must be given this information.

The person who collects data will often not be the same as the controller of the file in which the data will eventually be stored and processed. In order that he may assert his rights against the latter, it is important that the data subject should be informed of his name and address when the data are collected.

Article 13(2) empowers the Member States to restrict the duty to inform the data subject at the time of collection of data on grounds of the existence of predominant general interests. Under this provision, there is no duty to supply the information mentioned in Article 13(1) to the data subject if the information prevents the proper discharge of the functions of public authorities entrusted with monitoring and supervisory duties or the maintenance of public order.

Article 14

Additional rights of data subjects

Article 14 of the Directive encompasses the rights of the data subject vis-à-vis the controller of the file. The purpose of data protection is to
safeguard the data subject's right to privacy. The rights of that party vis-à-vis the controller of the file therefore form a fundamental part of data protection.

Article 14(1) entitles the data subject to oppose the processing of data relating to him for legitimate reasons. Legitimate reasons, for the purposes of this provision, means the lack of a legal justification for processing personal data, e.g. because the requirement of Chapters II and III of the Directive as to the permissibility of such processing is not fulfilled with regard to a particular processing of data.

Article 14(2) safeguards the data subject against being made the subject of decisions by public- and private-sector institutions involving the assessment of human conduct on the sole basis of an automatic processing of personal data forming a data or personality profile of the data subject. This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his "data shadow".

If he is to assert effectively his rights to rectification, erasure or blocking of data vis-à-vis the controller of the file, it is essential that the data subject have access to the data in the file. This is granted to him by Article 14(3) and (4). Article 14(3) grants the data subject the right to be informed about the relevant facts relating to the processing of his personal data by the controller of the file so that he may assert his rights to rectification, erasure and blocking and exercise effective control over the processing of data relating to him. Article 14(4) confers on the data subject the right to obtain, at reasonable intervals and without excessive delay or expense, confirmation as to whether data on him are stored in the file and, if so, communication to him of those data in an intelligible form.

The provisions of Article 14(3) and (4) leave it to the Member States to
It is also left to the domestic law of the Member States to determine the meaning of the term "reasonable interval". Taking into consideration the interests of the data subject and of the controller of the file, the domestic law of the Member States may provide that the controller of the file may charge a data subject who exercises his right of access no more than the actual cost incurred. The charge must not be excessive.

Article 14(4) allows the Member States to lay down a special rule on the exercise of the data subject’s right of access where medical data are concerned. To protect the data subject from psychological shock, which in extreme cases may lead to suicide, such information might be provided to him by a medical expert.

Article 14(5) of the Directive grants the data subject the right to rectification, erasure or blocking of data if their processing is incompatible with the Directive.

The data subject may exercise the right to rectification if data relating to him are incorrect, incomplete, inaccurate, misleading or out of date. The right of the data subject to have data erased or blocked presupposes that they have been processed in violation of the Directive. Article 14(5) refers to all provisions of the Directive which regulate the collection, storage, processing and use of personal data.

The concept of blocking has its origins in the German Federal Data Protection Act (paras. 4, 27 and 35: Sperrung). If data are blocked because they have been collected, stored, processed or used in violation of the Directive’s rules, the controller of the file may still keep them stored in his file, but he is prohibited from processing or using them, and in particular from communicating them to third parties. The blocked data have to be marked in the file to inform users of the file of the blocking.

The wording of the Directive ("as the case may be") leaves the precise shaping of the data subject’s rights of erasure, blocking or rectification with regard to the different situations in which personal data are processed and used in violation of the Directive to the data protection legislation of the Member States.
Frequently, data are not only processed by a controller of a file, but communicated to third parties. If the controller of the file has to rectify, erase or block data because they are incorrect or unlawfully processed or used, it is in the data subject's interest that third parties to whom such data have been transmitted should be notified of the rectification, erasure or blocking so that they, too, can rectify, erase or block the data. This interest of the data subject is taken care of by Article 14(7).

Article 14(6) grants the data subject the right to have data concerning him erased from files which serve marketing and direct-mail advertising purposes. The data subject can thus protect himself against unsolicited direct-mail advertising.

Finally, Article 14(8) obliges the Member States to grant the data subject an effective judicial remedy should the controller of the file or another person infringe his rights as set out in Article 14.

**Article 15**

*Exceptions to the data subject's right of access to public-sector files*

Article 15 authorizes the Member States to restrict the data subject's right of access to data files in order to protect an overriding public interest or an interest of a private individual equivalent to the data subject's right to privacy where the files are held by the public sector.

It is left to the Member States to decide to what extent they include in their domestic data protection legislation exceptions based on Article 15. However, the exceptions set out in this provision are limited to those necessary for the safeguarding of substantial values in a democratic society and have to be adopted by a formal statute. The list of interests which justify a restriction of the right of access under Article 15 of the Directive is exhaustive.
The term "national security" is to be interpreted as meaning the protection of national sovereignty against internal and external threats.

"Criminal proceedings" covers the prosecution of crimes which have already been committed, whereas the concept of "public safety" encompasses all the policing functions of state organs including crime prevention. The phrase "substantial economic and financial interests of a Member State or of the European Communities" refers to all economic policy measures and means of financing the policies of a Member State or of the Community, e.g. exchange controls, foreign trade controls and tax collection. However, only a substantial interest of this kind justifies a restriction of the right of access.

Finally, an interest of a third party equivalent to the data subject's right of access or the rights and freedoms of others are considered valid grounds for restricting the right of access. Such interests include the trade secrets of others or the freedom of the press.

If the data subject is denied access to data relating to him contained in a file because an interest covered by Article 15(1) is involved, the data protection authority, at his request, must carry out the necessary inspection and checks on the file in which the data are stored.

Article 15(3) empowers the Member States to place limits on the right of access to data compiled only temporarily for the purpose of extracting statistical information, as such operations pose only a minor threat to the data subject.
Chapter V

Data quality

The data protection principles set forth in this Chapter are more far reaching than its title suggests: they cover not only the quality of data (Article 16), but also the processing of certain categories of data which are considered to be particularly sensitive from the point of view of the interests of the data subject (Article 17) and the appropriate data security measures (Article 18).

Article 16

Principles

Article 16 of the Directive requires the Member States to incorporate the basic principles relating to the quality of personal data in their domestic data protection legislation. These principles are designed to safeguard the data subject's right to privacy by placing certain restrictions on the collection and processing of personal data and on the permissible contents of personal data files.

Article 16(1)(a) requires that the collection and processing of personal data should be carried out fairly and lawfully.

This provision covers the processing of personal data as defined in Article 2(d) as well as its gathering.

Article 16(1)(a) rules out, say, the use of technical devices hidden from the data subject which serve to obtain data secretly and without his knowledge, for example by wire-tapping, eavesdropping and similar methods. It also prevents controllers of files from creating and using clandestine files containing personal data.
Article 16(1)(b) sets out the principle of "purpose specification". According to this principle, personal data may be stored only for specified, explicit and lawful purposes.

The purpose for which personal data are stored must be specific in that the aim which the storage and use of the data is intended to serve must be defined and specified in as narrow terms as possible. A general or vague definition or description of the purpose of a file (e.g., the file is intended to serve "business purposes") will not be consonant with the purpose specification principle as laid down in Article 16(1)(b). The purpose has to be specified before the storage is effected. Where the data are collected from the data subject, the purpose should be specified at the time of collection (cf. Article 13).

Subsequent changes in the purpose of processing are permissible only in so far as they are not incompatible with its former purpose.

Article 16(1)(b) also requires that the controller of the file should make the purpose of storage and use of the data explicit. The requirement of explicitness seeks to prevent personal data from being stored and used for hidden purposes.

The requirement of lawfulness of the purpose of storage and use of personal data limits the potential purposes which a data file may serve; a file may be created and used only for purposes which are compatible with this Directive and the domestic law of the Member States. Furthermore, only such purposes as are relevant to the administrative functions of controllers of files in the public sector and the business activities of controllers of files in the private sector are lawful. Article 16(1)(b) states clearly that the purpose specification principle applies not only to the processing of personal data: the use of such data also has to be compatible with the purpose of the file.

Article 16(1)(c) provides that the data in a file must be adequate, relevant and not excessive in relation to the purposes for which they are stored. This principle seeks to ensure that the contents of a file are in keeping with its purpose.
Standing in close relationship with the requirements of Article 16(1)(b) and (c) are the provisions of Article 16(1)(d). Personal data stored in a file have to be accurate and, if necessary, kept up to date. If data are inaccurate or incomplete in relation to the purpose of the file, Article 16(1)(d) requires that they be erased or rectified.

Article 16(1)(e) deals with time limits for the retention of personal data. According to this provision, the keeping of data in a form which permits identification of the data subject is allowed only for as long as is necessary for the purposes for which the data are stored.

There may be circumstances however, in which it is necessary, e.g. for statistical purposes, to keep data beyond that time limit. It is essential, in such circumstances, for the protection of the data subject that the link between his name and the data be removed.

Article 16(2) makes it the duty of the controller of the file to ensure that the data quality provisions of Article 16(1) are complied with.

Article 17

Special categories of data

It is generally accepted that the right to privacy is endangered, not by the contents of personal data, but by the context in which the processing of personal data takes place. However, there is a broad consensus among the Member States that there are certain categories of data which, by virtue of their contents – quite irrespective of the context in which they are processed – carry the risk of infringing the data subject's right to privacy. Article 17 of the Directive therefore places strict limits on the electronic processing and use of sensitive information in personal data files.
Article 17 classes as sensitive the following categories of data: racial origin (including information on skin colour); political opinions, religious beliefs and philosophical convictions, including the fact that a person holds no religious belief (these categories encompass information on activities of the data subject relating to political, religious or philosophical convictions); information on trade-union membership; information on the data subject's health (including information on his past, present and future state of physical and mental health and information on drug and alcohol abuse); information concerning sexual life.

As a general rule, Article 17(1) prohibits the automatic processing of sensitive data. Exceptions to this rule are processing with the consent of the data subject, which has to be freely given, express and declared in writing, and the exception set out in Article 17(2).

According to the latter provision, the Member States may allow the electronic processing of sensitive data if it is required on important public interest grounds. However, such an exception presupposes as a legal basis the adoption of a formal statute specifying the kinds of sensitive data which may be processed electronically and the persons who may have access to the data, and providing appropriate safeguards against abuse and unauthorized access.

Article 17(3) covers the special case of the storage of information on criminal convictions. The storage of such information is permitted only in public-sector data files.

The scope of Article 17 is limited to data processed by automated means.

The article does not cover the electronic storage and processing of data on political opinions, religious and philosophical convictions and trade-union membership where such data are processed by non-profit-making organizations in accordance with Article 3(2)(b).
Article 18

Data security

Threats to the data subject's right to privacy do not emanate only from the controller of the file, who collects, stores, processes and communicates the individual's data for his own purposes.

His right to privacy is also jeopardized if his data are misused by third parties through unauthorized access to and use of the data.

The first sentence of Article 18(1) requires the Member States to oblige the controller of the file to take appropriate organizational and technical measures to protect the data in the file against the danger of unauthorized intrusion by third parties into a file or accidental loss of data, including accidental or unauthorized destruction, unauthorized modification of or access to data and any other unauthorized processing.

Technical measures of data security include: safety measures for access to data processing and storage locations, identification codes for persons entitled to enter such locations, informational safeguards such as the use of passwords for access to electronically processed files, the enciphering of data and monitoring of hacking and other unusual activities. Through organizational measures, the controller of the file adopts certain procedural steps within the hierarchy of his public authority or business enterprise, e.g. by establishing authority levels with regard to access to the data.

The second sentence of Article 18(1) lays down the standard of appropriate data security measures with regard to automated data files. The measures have to ensure an appropriate level of security having regard to the state
of the art in the field of data security, the cost of taking those measures, the nature of the data stored in the file and the assessment of the potential risks. In order to determine the appropriateness of data security measures, the controller of the file has to take into consideration any recommendations on data security and network interoperability formulated by the Community in accordance with Article 29 of the Directive.

The obligation to take appropriate security measures is not limited to the location of the data processing or of the hardware and software used for the processing. If data transmissions take place between one computer and another or between a computer and terminals via a telecommunications network, according to Article 18(2) security measures also have to be taken with regard to the network in order to guarantee the safe and uninterrupted transfer of data.

Article 18(3) covers the case of direct access by a remote user to a file via on-line retrieval. The authority of the user to obtain data from the file is specified in and limited by the contract with the controller of the file. The Directive requires the controller of the file to design hardware and software used for on-line retrieval in such a way that the user’s access remains within the limits of the authorization granted to him by the controller of the file.

Article 18(4) assigns responsibility for compliance with the obligations laid down by Article 18(1) to (3). The persons who - de facto or by contract - control the operations relating to a data file are also responsible for ensuring compliance with the data security requirements. Those to whom this rule applies are, as the case may be, the controller of the file, the user having access via on-line data retrieval and data processing service bureaux performing data processing operations on behalf of the controller of the file.
Finally, Article 18(5) places a duty of professional secrecy on employees of the controller of a file and other persons who in the course of their professional activities have access to the personal information in a file. These persons are prohibited from communicating the information to which they have access to third parties without the authorization of the controller of the file.

CHAPTER VI

Provisions specifically relating to certain sectors

Article 19

The Member States may provide for derogations from the Directive’s provisions in respect of the press, and the audiovisual media in so far as they are necessary in order to reconcile the fundamental rights of individuals, notably the right to privacy, with the freedom of information and of the press, there being a danger of conflict between the two categories of fundamental right. The approach adopted lays emphasis on the obligation to balance the interests involved in the event of a derogation. This balance may take into account, among other things, the availability to the data subject of remedies or of a right of reply, the existence of a code of professional ethics, the limits laid down by the European Convention on Human Rights and the general principles of law.

Article 20

This article provides that the Member States must encourage the business circles concerned to draw up codes of conduct or professional ethics so as to facilitate the application of the principles of the Directive in certain sectors. The Commission will also support such initiatives and will take them into account, if necessary, when it exercises its rule-making powers or puts forward new proposals.
CHAPTER VII

Liability and sanctions

Article 21
Liability

Where damage is suffered as a result of failure to comply with the Directive, liability rests under this article with the controller of the file, who may be sued by the data subject for compensation. The concept of damage covers both physical and non-physical damage. The liability of the controller of the file for loss, destruction or unauthorized access is limited if he can prove that the security requirements were complied with.

Article 22
Processing on behalf of the controller of the file

The object of this article is to avoid a situation whereby processing by a third party on behalf of the controller of the file has the effect of reducing the level of protection enjoyed by the data subject. To that end, obligations are placed both on the controller of the file and on the third party carrying out the processing.

Article 23
Sanctions

In order to ensure compliance with the measures taken pursuant to the Directive, the Member States are required to lay down truly dissuasive sanctions, such as criminal sanctions, bearing in mind, in particular, that non-compliance with the data protection principles constitutes an infringement of a fundamental right.
CHAPTER VIII

Transfer of personal data to third countries

Article 24
Principles

This article establishes the principle that the transfer of personal data from a Member State to a third country may take place only if that country ensures an adequate level of protection. It is for the Member States, and, if necessary, for the Commission, to determine whether a country ensures an adequate level of protection. The Member States must inform the Commission of cases in which an importing third country does not ensure such a level of protection. In that event, negotiations may be entered into between the Commission and the third country concerned.

The Commission may decide, in the exercise of the implementing powers conferred on it by Article 29, that a country ensures an adequate level of protection in the light of its domestic law and/or of the international commitments it has entered into. The Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data forms part of the commitments which the Commission will take into account. It may also draw on the expertise of the Working Party on the Protection of Personal Data in this field.

Article 25
Derogation

If a country does not ensure an adequate level of protection, a derogation permitting the transfer of data is possible in respect of a given export. The Member State in which the file is located may authorize such a transfer if the controller of the file can guarantee an adequate level of protection in respect of that export and if neither the other Member States nor the Commission object. To that end an information procedure is provided for, with a ten-day period in which notice of opposition may be given.
Where notice of opposition is given, the Commission may take the appropriate measures, including prohibition of the transfer.

CHAPTER IX

Supervisory authorities and the Working Party on the Protection of Personal Data

Article 26
Supervisory authority

This article provides for the setting-up of a supervisory authority characterized by its independence and by powers of investigation and intervention suited to the performance of the supervisory duties entrusted to it. National law must guarantee these two characteristics. The term "supervisory authority" does not prejudice the adoption of a multiple internal structure based on the constitutional system of the Member States.

Article 27
Working Party on the Protection of Personal Data

Owing to the special features of the protection of individuals in relation to personal data, this article sets up a working party of an advisory nature, the Working Party on the Protection of Personal Data. The Working Party on the Protection of Personal Data is characterized by its independence and is composed of representatives of the national supervisory authorities. The Working Party is chaired by a representative of the Commission.

Article 28
Tasks of the Working Party on the Protection of Personal Data

This article sets out the tasks of the Working Party on the Protection of Personal Data. The Working Party gives the Commission the benefit of its
knowledge and expertise in the field of the protection of individuals in relation to the processing of personal data, thereby contributing to the uniform application of the national rules adopted pursuant to the Directive; it assesses the level of protection in the Community and in third countries and informs the Commission thereof; and it may advise the Commission on any additional measures that need to be taken.

The Working Party on the Protection of Personal Data may formulate recommendations which may, if it so wishes, be transmitted to the Advisory Committee that is consulted by the Commission in the exercise of its implementing powers.

An annual report on the situation regarding the protection of personal data in the Community and in third countries is drawn up by the Working Party on the Protection of Personal Data. The report is transmitted to the Commission.

CHAPTER X

Rule-making powers of the Commission

Articles 29 and 30

Exercise of rule-making powers

Advisory Committee

Article 29 confers on the Commission powers of execution in respect of the technical implementing measures that are necessary as a result of the extent and technical nature of the personal data processing field.

Since the Directive is designed to contribute to the completion of the internal market, Article 30 provides for the setting-up of an Advisory Committee to assist the Commission in the exercise of its implementing powers and applies the procedures laid down in the Council Decision of 13 July 1987 laying down the procedures for the exercise of implementing powers conferred on the Commission.
Proposal for a
COUNCIL DIRECTIVE
concerning the protection of individuals
in relation to the processing of personal data

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Articles 100a and 113 thereof,

Having regard to the proposal from the Commission,¹

In cooperation with the European Parliament,²

Having regard to the opinion of the Economic and Social Committee,³

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Single European Act, include establishing an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;
(2) Whereas the establishment and the functioning of an internal market in which, in accordance with Article 8a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely, regardless of the Member States in which they are processed or requested, but also that fundamental rights should be safeguarded in view of the increasingly frequent recourse in the Community to the processing of personal data in the various spheres of economic and social activity;

(3) Whereas the internal market comprises an area without frontiers; whereas, for that reason, the national authorities in the various Member States are increasingly being called upon, by virtue of the operation of Community law, to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State;

(4) Whereas the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(5) Whereas the difference in levels of protection of privacy in relation to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(6) Whereas in order to remove the obstacles to flows of personal data, the level of protection of privacy in relation to the processing of such data must be equivalent in all the Member States; whereas to that end it is necessary to approximate the relevant laws;
(7) Whereas the object of the national laws on the processing of personal
data is to protect fundamental rights, notably the right to privacy which is
recognized both in Article 8 of the Convention for the Protection of Human
Rights and Fundamental Freedoms and in the general principles of Community
law; whereas, for that reason, the approximation of those laws must not
result in any lessening of the protection they afford but must, on the
contrary, seek to ensure a high level of protection in the Community;

(8) Whereas the principles underlying the protection of privacy in relation
to the processing of personal data set forth in this Directive may be
supplemented or clarified, in particular as far as certain sectors are
concerned, by specific rules based on those principles;

(9) Whereas the protection principles must apply to all data files where
the activities of the controller of the file are governed by Community law;
whereas public-sector files which are not governed by Community law should,
as is provided for in the resolution of the representatives of the
Governments of the Member States of the European Communities meeting within
the Council of ..., be subject to the same protection principles set forth
in national laws; whereas, however, data files falling exclusively within
the confines of the exercise of a natural person's right to privacy, such
as personal address files, must be excluded;

(10) Whereas any processing of personal data in the Community should be
carried out in accordance with the law of the Member State in which the
data file is located so that individuals are not deprived of the protection
to which they are entitled under this Directive; whereas, in this
connection, each part of a data file divided among several Member States
must be considered a separate data file and transfer to a non-member
country must not be a bar to such protection;

(11) Whereas any processing of personal data must be lawful; whereas such
lawfulness must be based on the consent of the data subject or on Community
or national law;
(12) Whereas national laws may, under the conditions laid down in this Directive, specify rules on the lawfulness of processing; whereas, however, such a possibility cannot serve as a basis for supervision by a Member State other than the State in which the data file is located, the obligation on the part of the latter to ensure, in accordance with this Directive, the protection of privacy in relation to the processing of personal data being sufficient, under Community law, to permit the free flow of data;

(13) Whereas the procedures of notification, in respect of public- or private-sector data files, and provision of information at the time of first communication, in respect of private-sector data files, are designed to ensure the transparency essential to the exercise by the data subject of the right of access to data relating to him;

(14) Whereas the data subject must, if his consent is to be valid and when data relating to him are collected from him, be given accurate and full information;

(15) Whereas the data subject must be able to exercise the right of access in order to verify the lawfulness of the processing of data relating to him and their quality;

(16) Whereas, if data are to be processed, they must fulfill certain requirements; whereas the processing of data which are capable by their very nature of infringing the right to privacy must be prohibited unless the data subject gives his explicit consent; whereas, however, on important public interest grounds, notably in relation to the medical profession, derogations may be granted on the basis of a law laying down precisely and strictly the conditions governing and limits to the processing of this type of data;

(17) Whereas the protection of privacy in relation to personal data requires that appropriate security measures be taken, both at the level of design and at that of the techniques of processing, to prevent any unauthorized processing;
(18) Whereas as regards the media the Member States may grant derogations from the provisions of this Directive in so far as they are designed to reconcile the right to privacy with the freedom of information and the right to receive and impart information, as guaranteed, in particular, in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

(19) Whereas the Member States must encourage the drawing-up, by the business circles concerned, of European codes of conduct or professional ethics relating to certain specific sectors; whereas the Commission will support such initiatives and will take them into account when it considers the appropriateness of new, specific measures in respect of certain sectors;

(20) Whereas, in the event of non-compliance with this Directive, liability in any action for damages must rest with the controller of the file; whereas dissuasive sanctions must be applied in order to ensure effective protection;

(21) Whereas it is also necessary that the transfer of personal data should be able to take place with third countries having an adequate level of protection; whereas, in the absence of such protection in third countries, this Directive provides, in particular, for negotiation procedures with those countries;

(22) Whereas the principles contained in this Directive give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(23) Whereas the existence in each Member State of an independent supervisory authority is an essential component of the protection of individuals in relation to the processing of personal data; whereas at Community level, a Working Party on the Protection of Personal Data,
must be set up and be completely independent in the performance of its functions; whereas having regard to its specific nature it must advise the Commission and contribute to the uniform application of the national rules adopted pursuant to this Directive;

(24) Whereas the adoption of additional measures for applying the principles set forth in this Directive calls for the conferment of rule-making powers on the Commission and the establishment of an Advisory Committee in accordance with the procedures laid down in Council Decision (1) 87/373/EEC,

HAS ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. The Member States shall ensure, in accordance with this Directive, the protection of the privacy of individuals in relation to the processing of personal data contained in data files.

2. The Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons to do with the protection afforded under paragraph 1.

(1) OJ No L 197, 18.7.1987, p. 33.
Article 2

Definitions

For the purposes of this Directive:

(a) "personal data" means any information relating to an identified or identifiable individual ("data subject"); an identifiable individual is notably an individual who can be identified by reference to an identification number or a similar identifying particular;

(b) "depersonalize" means modify personal data in such a way that the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time;

(c) "personal data file" (file) means any set of personal data, whether centralized or geographically dispersed, undergoing automatic processing or which, although not undergoing automatic processing, are structured and accessible in an organized collection according to specific criteria in such a way as to facilitate their use or combination;

(d) "processing" means the following operations, whether or not performed by automated means: the recording, storage or combination of data, and their alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure;

(e) "controller of the file" means the natural or legal person, public authority, agency or other body competent under Community law or the national law of a Member State to decide what will be the purpose of the file, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them;
(f) "supervisory authority" means the independent public authority or other independent body designated by each Member State in accordance with Article 26 of this Directive;

(g) "public sector" means all the authorities, organizations and entities of a Member State that are governed by public law, with the exception of those which carry on an industrial or commercial activity, and bodies and entities governed by private law where they take part in the exercise of official authority;

(h) "private sector" means any natural or legal person or association, including public-sector authorities, organizations and entities in so far as they carry on an industrial or commercial activity.

Article 3

Scope

1. The Member States shall apply this Directive to files in the public and private sectors with the exception of files in the public sector where the activities of that sector do not fall within the scope of Community law.

2. This Directive shall not apply to files held by:

(a) an individual solely for private and personal purposes; or

(b) non-profit-making bodies, notably of a political, philosophical, religious, cultural, trade-union, sporting or leisure nature, as part of their legitimate aims, on condition that they relate only to those members and corresponding members who have consented to being included therein and that they are not communicated to third parties.
Article 4

Law applicable

1. Each Member State shall apply this Directive to:

(a) all files located in its territory;

(b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.

2. Each Member State shall apply Articles 5, 6, 8, 9, 10, 17, 18 and 21 of this Directive to a user consulting a file located in a third country from a terminal located in the territory of a Member State, unless such use is only sporadic.

3. Where a file is moved temporarily from one Member State to another, the latter shall place no obstacle in the way and shall not require the completion of any formalities over and above those applicable in the Member State in which the file is normally located.
CHAPTER 11

LAWFULNESS OF PROCESSING IN THE PUBLIC SECTOR

Article 5

Principles

1. Subject to Article 6, the Member States shall, with respect to files in the public sector, provide in their law that:

(a) the creation of a file and any other processing of personal data shall be lawful in so far as they are necessary for the performance of the tasks of the public authority in control of the file;

(b) the processing of data for a purpose other than that for which the file was created shall be lawful if:
   - the data subject consents thereto; or
   - it is effected on the basis of Community law, or of a law, or a measure taken pursuant to a law, of a Member State conforming with this Directive which authorizes it and defines the limits thereto; or
   - the legitimate interests of the data subject do not preclude such change of purpose; or
   - it is necessary in order to ward off an imminent threat to public order or a serious infringement of the rights of others.

Article 6

Processing in the public sector having as its object the communication of personal data

1. The Member States shall provide in their law that the communication of personal data contained in the files of a public-sector entity shall be lawful only if:
(a) It is necessary for the performance of the tasks of the public-sector entity communicating or requesting communication of the data; or

(b) It is requested by a natural or legal person in the private sector who invokes a legitimate interest, on condition that the interest of the data subject does not prevail.

2. Without prejudice to paragraph 1, the Member States may specify the conditions under which the communication of personal data is lawful.

3. The Member States shall provide in their law that, in the circumstances referred to in paragraph 1(b), the controller of the file shall inform data subjects of the communication of personal data. The Member States may provide for the replacing of such provision of information by prior authorization by the supervisory authority.

Article 7

Obligation to notify the supervisory authority

1. The Member States shall provide in their law that the creation of a public-sector file the personal data in which might be communicated shall be notified in advance to the supervisory authority and recorded in a register kept by that authority. The register shall be freely available for consultation.

2. The Member States shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file; the purpose of the file; a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3. The Member States may provide that paragraphs 1 and 2 shall apply to other public-sector files and that consultation of the register may be restricted for the reasons stated in Article 15(1).
CHAPTER III

LAWFULNESS OF PROCESSING IN THE PRIVATE SECTOR

Article 8

Principles

1. The Member States shall provide in their law that, without the consent of the data subject, the recording in a file and any other processing of personal data shall be lawful only if it is effected in accordance with this Directive and if:

(a) the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge; or

(b) the data come from sources generally accessible to the public and their processing is intended solely for correspondence purposes; or

(c) the controller of the file is pursuing a legitimate interest, on condition that the interest of the data subject does not prevail.

2. The Member States shall provide in their law that it shall be for the controller of the file to ensure that no communication is incompatible with the purpose of the file or is contrary to public policy. In the event of on-line consultation, the same obligations shall be incumbent on the user.

3. Without prejudice to paragraph 1, the Member States may specify the conditions under which the processing of personal data is lawful.
Article 9

Obligation to inform the data subject

1. The Member States shall, with respect to the private sector, provide in their law that at the time of first communication or of the affording of an opportunity for on-line consultation the controller of the file shall inform the data subject accordingly, indicating also the purpose of the file, the types of data stored therein and his name and address.

2. The provision of information under paragraph 1 shall not be mandatory in the circumstances referred to in Article 8(1)(b). There shall be no obligation to inform where communication is required by law.

3. If the data subject objects to communication or any other processing, the controller of the file shall cease the processing objected to unless he is authorized by law to carry it out.

Article 10

Special exceptions to the obligation to inform the data subject

If the provision of information to the data subject provided for in Article 9(1) proves impossible or involves a disproportionate effort, or comes up against the overriding legitimate interests of the controller of the file or a similar interest of a third party, the Member States may provide in their law that the supervisory authority may authorize a derogation.
Article 11

Obligation to notify the supervisory authority

1. The Member States shall provide in their law that the controller of the file shall notify the creation of a personal data file where the data are intended to be communicated and do not come from sources generally accessible to the public. The notification shall be made to the supervisory authority of the Member State in which the file is located or, if it is not located in a Member State, to the supervisory authority of the Member State in which the controller of the file resides. The controller of the file shall notify to the competent national authorities any change in the purpose of the file or any change in his address.

2. The Member States shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3. The Member States may provide that paragraphs 1 and 2 shall apply to other private-sector files and that the information referred to in paragraph 2 shall be accessible to the public.
CHAPTER IV

RIGHTS OF DATA SUBJECTS

Article 12

Informed consent

Any giving of consent by a data subject to the processing of personal data relating to him within the meaning of this Directive shall be valid only if:

(a) the data subject is supplied with the following information:
   - the purposes of the file and the types of data stored;
   - the type of use and, where appropriate, the recipients of the personal data contained in the file;
   - the name and address of the controller of the file;

(b) it is specific and express and specifies the types of data, forms of processing and potential recipients covered by it;

(c) it may be withdrawn by the data subject at any time without retroactive effect.

Article 13

Provision of Information at the time of collection

1. The Member States shall guarantee individuals from whom personal data are collected the right to be informed at least about:
   (a) the purposes of the file for which the information is intended;
   (b) the obligatory or voluntary nature of their reply to the questions to which answers are sought;
   (c) the consequences if they fail to reply;
   (d) the recipients of the information;
   (e) the existence of the right of access to and rectification of the data relating to them; and
   (f) the name and address of the controller of the file.
2. Paragraph 1 shall not apply to the collection of information where to inform the data subject would prevent the exercise of the supervision and verification functions of a public authority or the maintenance of public order.

**Article 14**

**Additional rights of data subjects**

The Member States shall grant a data subject the following rights:

1. To oppose, for legitimate reasons, the processing of personal data relating to him.

2. Not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality.

3. To know of the existence of a file and to know its main purposes and the identity and habitual residence, headquarters or place of business of the controller of the file.

4. To obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in a file and communication to him of such data in an intelligible form.

The Member States may provide that the right of access to medical data may be exercised only through a doctor.

5. To obtain, as the case may be, rectification, erasure or blocking of such data if they have been processed in violation of the provisions of this Directive.
6. To obtain upon request and free of charge the erasure of data relating to him held in files used for market research or advertising purposes.

7. To obtain, in the event of the application of paragraph 5 and if the data have been communicated to third parties, notification to the latter of the rectification, erasure or blocking.

8. To have a judicial remedy if the rights guaranteed in this Article are infringed.

Article 15

Exceptions to the data subject's right of access to public-sector files

1. The Member States may limit by statute the rights provided for in points 3 and 4 of Article 14 for reasons relating to:

   (a) national security,
   (b) defence,
   (c) criminal proceedings,
   (d) public safety,
   (e) a duly established paramount economic and financial interest of a Member State or of the European Communities,
   (f) the need for the public authorities to perform monitoring or inspection functions, or
   (g) an equivalent right of another individual and the rights and freedoms of others.

2. In the circumstances referred to in paragraph 1, the supervisory authority shall be empowered to carry out, at the request of the data subject, the necessary checks on the file.

3. The Member States may place limits on the data subject's right of access to data compiled temporarily for the purpose of extracting statistical information therefrom.
CHAPTER V

DATA QUALITY

Article 16

Principles

1. The Member States shall provide that personal data shall be:

(a) collected and processed fairly and lawfully;
(b) stored for specified, explicit and lawful purposes and used in a way compatible with those purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
(d) accurate and, if necessary, kept up to date; inaccurate or incomplete data shall be erased or rectified;
(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which the data are stored.

2. It shall be for the controller of the file to ensure that paragraph 1 is complied with.
Article 17

Special categories of data

1. The Member States shall prohibit the automatic processing of data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs or trade-union membership, and of data concerning health or sexual life, without the express and written consent, freely given, of the data subject.

2. The Member States may, on important public interest grounds, grant derogations from paragraph 1 on the basis of a law specifying the types of data which may be stored and the persons who may have access to the file and providing suitable safeguards against abuse and unauthorized access.

3. Data concerning criminal convictions shall be held only in public-sector files.

Article 18

Data security

1. The Member States shall provide in their law that the controller of a file shall take appropriate technical and organizational measures to protect personal data stored in the file against accidental or unauthorized destruction or accidental loss and against unauthorized access, modification or other processing.
Such measures shall ensure, in respect of automated files, an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks. To that end, the controller of the file shall take into consideration any recommendations on data security and network interoperability formulated by the Commission in accordance with the procedure provided for in Article 29.

2. Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network.

3. In the event of on-line consultation, the hardware and software shall be designed in such a way that the consultation takes place within the limits of the authorization granted by the controller of the file.

4. The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who, either de facto or by contract, control the operations relating to a file.

5. Any person who in the course of his work has access to information contained in files shall not communicate it to third parties without the agreement of the controller of the file.

CHAPTER VI

PROVISIONS SPECIFICALLY RELATING TO CERTAIN SECTORS

Article 19

The Member States may grant, in respect of the press and the audiovisual media, derogations from the provisions of this Directive in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press.
Article 20

The Member States shall encourage the business circles concerned to participate in drawing up European codes of conduct or professional ethics in respect of certain sectors on the basis of the principles set forth in this Directive.

CHAPTER VII

LIABILITY AND SANCTIONS

Article 21

Liability

1. The Member States shall provide in their law that any individual whose personal data have been stored in a file and who suffers damage as a result of processing or of any act incompatible with this Directive shall be entitled to compensation from the controller of the file.

2. The Member States may provide that the controller of the file shall not be liable for any damage resulting from the loss or destruction of data or from unauthorized access if he proves that he has taken appropriate measures to fulfill the requirements of Articles 18 and 22.

Article 22

Processing on behalf of the controller of the file

1. The Member States shall provide in their law that the controller of the file must, where processing is carried out on his behalf, ensure that the necessary security and organizational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.
2. Any person who collects or processes personal data on behalf of the controller of the file shall fulfill the obligations provided for in Articles 16 and 18 of this Directive.

3. The contract shall be in writing and shall stipulate, in particular, that the personal data may be divulged by the person providing the service or his employees only with the agreement of the controller of the file.

Article 23

Sanctions

Each Member State shall make provision in its law for the application of dissuasive sanctions in order to ensure compliance with the measures taken pursuant to this Directive.

CHAPTER VIII

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 24

Principles

1. The Member States shall provide in their law that the transfer to a third country, whether temporary or permanent, of personal data which are undergoing processing or which have been gathered with a view to processing may take place only if that country ensures an adequate level of protection.

2. The Member States shall inform the Commission of cases in which an importing third country does not ensure an adequate level of protection.
3. Where the Commission finds, either on the basis of information supplied by Member States or on the basis of other information, that a third country does not have an adequate level of protection and that the resulting situation is likely to harm the interests of the Community or of a Member State, it may enter into negotiations with a view to remedying the situation.

4. The Commission may decide, in accordance with the procedure laid down in Article 30(2) of this Directive, that a third country ensures an adequate level of protection by reason of the international commitments it has entered into or of its domestic law.

5. Measures taken pursuant to this Article shall be in keeping with the obligations incumbent on the Community by virtue of international agreements, both bilateral and multilateral, governing the protection of individuals in relation to the automatic processing of personal data.

**Article 25**

**Derogation**

1. A Member State may derogate from Article 24(1) in respect of a given export on submission by the controller of the file of sufficient proof that an adequate level of protection will be provided. The Member State may grant a derogation only after it has informed the Commission and the Member States thereof and in the absence of notice of opposition given by a Member State or the Commission within a period of ten days.

2. Where notice of opposition is given, the Commission shall adopt appropriate measures in accordance with the procedure laid down in Article 30(2).
CHAPTER IX

SUPERVISORY AUTHORITIES AND WORKING PARTY ON THE PROTECTION OF PERSONAL DATA

Article 26

Supervisory authority

1. The Member States shall ensure that an independent competent authority supervises the protection of personal data. The authority shall monitor the application of the national measures taken pursuant to this Directive and perform all the functions that are entrusted to it by this Directive.

2. The authority shall have investigative powers and effective powers of intervention against the creation and exploitation of files which do not conform with this Directive. To that end, it shall have, inter alia, the right of access to files covered by this Directive and shall be given the power to gather all the Information necessary for the performance of its supervisory duties.

3. Complaints in connection with the protection of Individuals in relation to personal data may be lodged with the authority by any individual.

Article 27

Working Party on the Protection of Personal Data

1. A Working Party on the Protection of Personal Data is hereby set up. The Working Party, which shall have advisory status and shall act independently, shall be composed of representatives of the supervisory authorities provided for in Article 26 of all the Member States and shall be chaired by a representative of the Commission.
2. The secretariat of the Working Party on the Protection of Personal Data shall be provided by the Commission's departments.


4. The Working Party on the Protection of Personal Data shall examine questions placed on the agenda by its chairman, either on his own initiative or at the reasoned request of a representative of the supervisory authorities, concerning the application of the provisions of Community law on the protection of personal data.

**Article 28**

**Tasks of the Working Party on the Protection of Personal Data**

1. The Working Party on the Protection of Personal Data shall:
   (a) contribute to the uniform application of the national rules adopted pursuant to this Directive;
   (b) give an opinion on the level of protection in the Community and in third countries;
   (c) advise the Commission on any draft additional or specific measures to be taken to safeguard the protection of privacy.

2. If the Working Party on the Protection of Personal Data finds that significant divergences are arising between the laws or practices of the Member States in relation to the protection of personal data which might affect the equivalence of protection in the Community, it shall inform the Commission accordingly.

3. The Working Party on the Protection of Personal Data may formulate recommendations on any questions concerning the protection of individuals in relation to personal data in the Community. The recommendations shall be recorded in the minutes and may be transmitted to the Advisory Committee referred to in Article 30. The Commission shall inform the Working Party on the Protection of Personal Data of the action it has taken in response to the recommendations.
4. The Working Party on the Protection of Personal Data shall draw up an annual report on the situation regarding the protection of individuals in relation to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission.

CHAPTER X

RULE-MAKING POWERS OF THE COMMISSION

Article 29

Exercise of rule-making powers

The Commission shall, in accordance with the procedure laid down in Article 30(2), adopt such technical measures as are necessary to apply this Directive to the specific characteristics of certain sectors having regard to the state of the art in this field and to the codes of conduct.

Article 30

Advisory Committee

1. The Commission shall be assisted by a committee of an advisory nature composed of the representatives of the Member States and chaired by a representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter, if necessary by taking a vote. The opinion shall be recorded in the minutes; in addition, each Member State shall have the right to ask to have its position recorded in the minutes. The Commission shall take the utmost account of the opinion delivered by the committee. It shall inform the committee of the manner in which its opinion has been taken into account.
FINAL PROVISIONS

Article 31

1. The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 1 January 1993.

The provisions adopted pursuant to the first subparagraph shall make express reference to this Directive.

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

Article 32

The Commission shall report to the Council and the European Parliament at regular intervals on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments.

Article 33

This Directive is addressed to the Member States.

Done at Brussels, For the Council
Fiche Financière

PROPOSITION DE DIRECTIVE DU CONSEIL
VISANT AU RAPPROCHEMENT DE CERTAINES DISPOSITIONS
LEGISLATIVES, RÉGLEMENTAIRES ET ADMINISTRATIVES
DES ÉTATS MEMBRES
RELATIVES À LA PROTECTION DES PERSONNES
À L'ÉGARD DU TRAITEMENT DES DONNÉES
À CARACTÈRE PERSONNEL

1. Ligne budgétaire concernée (éventuellement à créer) :

A 2511 : Frais de réunions de comités dont la consultation n'est pas un élément obligatoire de la procédure de formation d'actes communautaires.

2. Base légale (ou autre) :

Article 100 A

3. Proposition de classification en dépense obligatoire/non obligatoire

(avec justification succincte en vertu de la déclaration commune du 30 juin 1982) :

non-obligatoire

4. Description et justification de l'action :

4.1. Objectifs :
- assurer la protection des personnes à l'égard des données à caractère personnel,
- permettre la circulation transfrontière de données à caractère personnel dans la Communauté,
- permettre le bon fonctionnement du marché intérieur.

4.2. Création de 2 comités compétents en matière de protection des personnes à l'égard des données à caractère personnel (Art. 27, 30)

personnes concernées : 1. Pour le Comité de protection des données à caractère personnel (Art. 27) :
représentants de l'autorité de contrôle de tous les États membres (groupe 4)

2. Pour le Comité consultatif (Art. 30) :
représentants des États membres (groupe 3)

4.3. Un représentant de la Commission préside le Comité de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du Comité de protection des données à caractère personnel est assuré par les services de la Commission.
5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions
(frais de participation des membres des 2 Comités)

5.2. Calcul :
- Comité de protection des données :
  24 membres (non-gouvernementals) x 3 réunions
  a 2 jours x 1180 ECU (590 ECU/Jour) = 84.960 ECU*
- Comité consultatif :
  24 membres (gouvernemental) x 1 réunion a 2 jours x
  780 ECU (390 ECU/Jour) = 18.720 ECU*

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancler des crédits d'engagement et de paiement

  CE-CP
  
  1993 : 103.680 ECU
  1994 : 
  1995 : 
  1996 : 
  1997 : 

6.2. Part du financement communautaire dans le coût total : 100%

7. Observations :

1. Le Comité de protection des données à caractère personnel (Art. 27) :

   Il est institué ce Comité à caractère consultatif et indépendant et
   est composé de représentants de l'autorité de contrôle de tout les
   Etats membres, présidé par un représentant de la Commission.

   Ce Comité établit son règlement intérieur. Le secrétariat du Comité
   est assuré par les services de la Commission.

   Missions de ce Comité : voir Art.28.

2. Le Comité consultatif (Art.30) :

   Il est institué un Comité consultatif composé des représentants des
   Etats membres, présidé par le représentant de la Commission.

   La Commission est assistée par ce Comité afin de prendre les
   éventuelles mesures complémentaires nécessaires pour adapter les
   dispositions de la directive aux spécificités de certaines secteurs.

* estimation
FICHE D'IMPACT SUR LA COMPETITIVITE ET L'EMPLOI

I. Quelle est la justification principale de la mesure ?

- Assurer la protection des personnes à l'égard des données à caractère personnel.
- Permettre la circulation transfrontière de données à caractère personnel dans la Communauté.
- Permettre le bon fonctionnement du marché intérieur.

II. Caractéristiques des entreprises concernées.

La proposition concerne toutes les entreprises qui utilisent des fichiers de données à caractère personnel quel que soit leur taille ou leur secteur d'activité.

III. Quelles sont les obligations imposées directement aux entreprises ?

Se conformer aux dispositions applicables aux traitements de données à caractère personnel, notamment celles relatives à la légitimité de ces traitements dans le secteur privé.

IV. Quelles sont les obligations susceptibles d'être imposées indirectement aux entreprises via les autorités locales ?

Aucune.

V. Y a-t-il des mesures spéciales pour les PME ?

Non.
VI. Quel est l’effet prévisible ?

a) sur la compétitivité des entreprises ?

Les règles de protection s’appliquent à toutes les entreprises et élimineront les distorsions de concurrence dues à l’actuelle disparité des législations nationales. En ce qui concerne leur compétitivité internationale, la directive prévoit des négociations avec les pays tiers qui n’assurent pas encore un niveau de protection adéquat.

b) sur l’emploi ?

La directive prévoit la création d’instances de contrôle nationales.

VII. Les partenaires sociaux ont-ils été consultés sur cette proposition ?

Non.
RESOLUTION OF THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES OF THE EUROPEAN COMMUNITIES MEETING WITHIN THE COUNCIL

THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES OF THE EUROPEAN COMMUNITIES MEETING WITHIN THE COUNCIL,

Whereas the Council Directive concerning the protection of individuals in relation to the processing of personal data ensures the protection of the privacy of individuals in relation to the processing of personal data contained in data files in the private and public sectors, with the exception of files in those parts of the public sector which do not fall within the scope of Community law,

Desirous to facilitate cooperation between the administrations of the Member States in sectors not falling within the scope of Community law while affording a high level of protection for the privacy of the persons affected,

Whereas the principles contained in the Directive give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data,

HEREBY ADOPT THIS RESOLUTION:

The Governments of the Member States undertake to apply the principles contained in the Council Directive concerning the protection of individuals in relation to the processing of personal data to those parts of the public sector which do not fall within the scope of Community law and to set in motion the necessary legislative procedures.
Commission Declaration on the application to the institutions and other
bodies of the European Communities of the principles contained in the
Council Directive concerning the protection of individuals in relation to
the processing of personal data

1. The Commission considers that the principles contained in the
Directive concerning the protection of individuals in
relation to the processing of personal data ("the Directive") must
apply to the institutions and other bodies of the European Communities.

2. To that end, the Commission will, at the earliest opportunity, take and
propose the necessary measures.

3. Pending the taking of such measures, the Commission undertakes to apply
the principles contained in the Directive to the processing of personal
data for which it is responsible.

4. The Commission considers that the other institutions of the
Communities must also undertake to apply the principles contained in the
Directive to the processing of personal data for which they are
responsible.
PROPOSAL FOR A

COUNCIL DIRECTIVE

CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY IN THE
CONTEXT OF PUBLIC DIGITAL TELECOMMUNICATIONS NETWORKS,

IN PARTICULAR THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND
PUBLIC DIGITAL MOBILE NETWORKS
CONTENTS

A SUMMARY....................................................................................................................

B EXPLANATORY MEMORANDUM..............................................................................

I. Introduction ..................................................................................................................

II. The new specific requirements with regard to the protection of personal data and privacy in the telecommunications sector..........................................................................................................................

III. The approach proposed: the provisions of the draft Directive ..................................

IV. Conclusions ..................................................................................................................

PROPOSAL FOR A COUNCIL DIRECTIVE CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF PUBLIC DIGITAL TELECOMMUNICATIONS NETWORKS, IN PARTICULAR THE INTEGRATED SERVICES DIGITAL NETWORK(ISDN) AND PUBLIC DIGITAL MOBILE NETWORKS
A. SUMMARY

The introduction of public digital telecommunications networks is now fully under-way in the Community. During the early years of this decade more than 70% of long distance transmission, more than 50% of long distance switching and more than 30% of local switching will be digitalised.

The wide-spread introduction of public digital telecommunications networks in the Community will allow, in particular with the implementation of the Integrated Services Digital Network (ISDN) and the new digital mobile services, vastly enhanced telecommunications functions for the general public, but at the same time, will require a Community-wide common approach for the protection of privacy, personal data and data security with regard to the specific requirements of the new digital telecommunications environment.

The Council and the European Parliament have recognised repeatedly the central role of adequate measures concerning data protection and protection of privacy for the future development of telecommunications in the European Community. In particular, in its resolutions of 14 December 1988 on telecommunications, the European Parliament called for specific measures "to ensure data privacy protection and confidentiality" and reminded the Commission "of its political responsibility for ensuring that legislative proposals on opening up telecommunications markets, in the appropriate legal form, are accompanied by action at Community level relating to the protection of personal data".

In the Community, there is growing attention paid to the impact of digital networks on the protection of personal data and privacy. In a resolution adopted at Berlin in August 1989, the data protection commissioners of the Member States called for special attention with regard to protection of personal data and privacy in the context of ISDN.

The enclosed proposal is intended to meet these specific requirements with regard to the protection of personal data and privacy in the field of the new public digital telecommunications networks. It is presented in the context of - and complementary to - the proposals by the Commission for the establishment of a general framework for data protection in the Community.

Effective protection of personal data and privacy is developing into an essential pre-
condition for social acceptance of the new digital networks and services. It must be an essential component of the Community's telecommunications policy which aims at securing for the European citizen the full benefits of advanced telecommunications services, as the Community moves towards an environment which will be substantially richer in information than before.

The enclosed proposal for a Council Directive has been drafted with this global objective in mind.
B. EXPLANATORY MEMORANDUM

I. INTRODUCTION

The current wide-spread introduction of public digital telecommunications in the Community, in particular the implementation of the Integrated Services Digital Network (ISDN)\(^1\) and new digital mobile services\(^2\) will allow vastly enhanced telecommunications functions for the general public, but at the same time, will require a Europe-wide common approach for the protection of privacy, personal data and data security with regard to the specific requirements of the new digital telecommunications environment.

In its Resolution on the coordinated introduction of the Integrated Services Digital Network in the European Community of 12 December 1986\(^3\), the European Parliament stated that the "prospective Integrated Services Digital Network (ISDN), evolving from the telephone network, will offer many additional services to corporate and private subscribers ..." but called on the Commission "to submit proposals on a practical approach towards ensuring within the ISDN now emerging throughout Europe, a consistent level of data-privacy protection commensurate with the enhanced technical capabilities of this new network". The European Parliament emphasised this concern further in a more general context in its resolutions of 14 December 1988\(^4\), where it called for specific measures with regard to the use of telecommunications networks "to ensure data-privacy protection and confidentiality" and reminded the Commission "of its political responsibility for ensuring that legislative proposals on opening up telecommunications markets, in the appropriate legal form, are accompanied by action at Community level relating to the protection of personal data ...".

---


The ISDN can be considered as a natural evolution of the telephone network. It will allow via a single access using the existing subscriber line, the transmission of voice (telephony), text, data, and images in the form of a multitude of more efficient or new services (for details see Council Recommendation 86/659/EEC and chapter ii.).

In accordance with the Council Recommendation, two progress reports on the implementation of ISDN were submitted up to now by the Commission (COM(88) 589; COM(90) 123).


4. Resolution on Posts and Telecommunications, OJ No C12, 16 January 1989, p. 69; resolution on the need to overcome the fragmentation in telecommunications, OJ No C 12, 16 January 1989, p. 66.
The Council in its resolution of 30 June 1988, by which it adopted the principles of the Green Paper on the development of the common market for telecommunications services and equipment and gave its general support to the objectives of the action programme set out in the communication of 9 February 1988 defined as one of the major policy goals "to protect personal data and to provide for the individual's access, through the communication media, to an environment significantly richer in information than before".

In its resolution on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992, the Council specified its concern further with regard to the ISDN by emphasising as necessary "further discussion at European level regarding user privacy protection requirements and requirements concerning the security of communications in the context of features of new services, in accordance with the resolution of the European Parliament of 12 December 1986 on recommendation 86/659/EEC".

The representatives of the authorities responsible for data protection in the Member States adopted at their 11th international conference on 28-31 August 1989 in Berlin a resolution calling for special attention with regard to the protection of data and privacy in the context of the ISDN.

With the enclosed proposal the Commission is responding to this requirement for specific Community-wide measures concerning the protection of personal data and privacy in the context of the implementation of the new public digital telecommunications networks, in particular the Integrated Services Digital Network and the public digital mobile networks. It takes account of the fact that there is deep and justified concern concerning the immediate impact of digital networks on the protection of personal data and privacy. The Commission has also recognised data protection and protection of privacy as an essential requirement in the context of the future development of an open network environment in the Community.

---


6 COM(87) 290.

7 Towards a competitive Community-wide telecommunications market in 1992: Implementing the Green Paper on the development of the common market for telecommunications services and equipment. State of discussions and proposals by the Commission (COM(88) 48).

8 OJ No C 196, 1 August 1989, p. 4.

9 Common position adopted by the Council on 5th February 1990 with a view to adopting a Directive on the establishment of the internal market for telecommunications services through the implementation of Open Network Provision (OJ.....).
The proposal must be seen against the background of discussions and the general principles established in Europe with regard to the protection of personal data through the Convention of the Council of Europe of 1981 for the Protection of Individuals with regard to Automated Processing of Personal Data, which has been ratified up to now by seven Member States of the Community. The proposal is presented in the context of - and complementary to - the proposals by the Commission for the establishment of a general framework for data protection in the Community submitted in parallel, in particular the draft Council Directive for the approximation of certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data, the draft Council Decision concerning the opening of negotiations in view of the adhesion of the European Economic Community, in the fields of its competence, to the Convention of the Council of Europe for the Protection of Individuals with regard to Automated Processing of Personal Data, and the draft Council Decision concerning the security of information systems; in addition, the Commission will develop internal rules with the objective to guarantee for the individuals concerned a level of protection equivalent to the principles of the Council Directive mentioned above.

Within this general context, the enclosed Directive is to provide for the specific provisions required for the approximation of laws, regulations and administrative provisions in the Community in the field of protection of personal data and privacy with regard to public fixed and mobile digital telecommunications networks and the new "intelligent" functions which they provide.
II. THE NEW SPECIFIC REQUIREMENTS WITH REGARD TO THE PROTECTION OF PERSONAL DATA AND PRIVACY IN THE TELECOMMUNICATIONS SECTOR

The "digitalisation" of the public telecommunications networks is now fully under way in the Community. During the early years of this decade more than 70% of long distance transmission, more than 50% of long distance switching and more than 30% of local switching will be digitalised.

Digitalisation means the introduction of fully computer-based exchanges and the processing and transmission of all information transmitted via telecommunications networks - voice, data and image - in the form of binary digits\textsuperscript{10}. The "bit-streams" thus generated can be acted upon directly by the intelligence of computers, both inside the network as well as in the subscriber terminal. This leads to a new level of quality of service which cannot be achieved with traditional "analogue" techniques, as well as a large number of new "intelligent" functions which opens a broad range of new activities via telecommunications networks. Full "end-to-end" (subscriber-to-subscriber) digital communication is offered by the evolving Integrated Services Digital Network and the new public digital mobile communications systems\textsuperscript{11}.

With regard to data protection, the introduction of public digital networks has two major consequences.

On the one hand, the fully computer-based techniques now possible can offer a substantially higher degree of data security for specific individual requirements, such as sophisticated encryption techniques.

On the other hand, due to the digital processing of both operational and call data and the treatment by computer-based exchanges, it could become possible - without adequate data protection measures - to store and monitor systematically specific call-related data, such as origin of call. Such a possibility was only feasible in traditional analogue-based "non-intelligent" networks by making a substantial technical effort and therefore was only implemented under very exceptional circumstances.

At the same time, the new intelligent telecommunications functions, such as defined by the ISDN "supplementary services"\textsuperscript{12}, offer substantial additional service features to the subscriber which will enhance service quality as well as consumer protection, such as detailed billing. The new functions, however, will require new specific measures and regulations, if the protection of privacy is to be guaranteed in the new environment.

\textsuperscript{10} Computers process all information in the form of "binary digits", i.e. by splitting all information into its fundamental information elements (bits) with values 0 or 1.


\textsuperscript{12} See for details Council Recommendation 86/659/EEC, footnote 1.
Therefore, the introduction of digital telecommunications networks in the Community gives rise, with regard to the protection of personal data, to substantial specific issues which must be addressed, such as the handling of:

- subscriber-related information, increasingly stored in computer-held subscriber files;
- traffic and other operational data;
- detailed billing data;
- calling-line identification (identification of origin of call);
- automatic call forwarding to third parties;
- unsolicited messages;
- specific technical features for terminal and other equipment which may be required, in order to provide for adequate protection.

The general provisions for protection of personal data, such as initiated by the Council of Europe convention and to be established for the Community by the Commission’s initiatives mentioned above, does provide a broad framework, but does not make provisions to the specific details required for addressing these issues.

The general provisions concerning the protection of personal data cannot prevent the current emergence of divergent legislation, regulations and administrative action in the Member States concerning the operation of the future digital networks which could very soon endanger the common market for both telecommunications services and terminal equipment.

For example, in the field of calling line identification, certain Member States plan to provide for a case-by-case elimination of the feature by the calling subscriber. If such an elimination will be realised via a button on the telephone set, while other operators might decide to provide for the elimination via a code to be used before dialling a number, it would create problems for the free circulation of terminal equipment in the Community.

A comparison of the existing national provisions shows considerable discrepancies concerning both the contents and the nature of the legal instruments used. Under these circumstances, a situation of legal uncertainty is developing in the Community concerning telecommunications networks and services, which threatens to hinder substantially the transborder offering of services.

Without a Directive concerning the specific provisions necessary to implement the general principles of protection of data and privacy with regard to public digital fixed and mobile networks, it would be impossible to prevent divergent developments in the Community.
At the same time, Community-wide provision for effective protection of personal data and privacy is developing into an essential pre-condition for social acceptance of the new digital networks and services, as confirmed by the Council at its meeting of 7 November 1989 where it concluded with regard to the social aspects of telecommunications on the need to preserve the protection of privacy and personal data within a European perspective.

The enclosed proposal for a Council Directive aims at fulfilling these specific requirements.
III. THE APPROACH PROPOSED: THE PROVISIONS OF THE DRAFT DIRECTIVE

The global objective of the proposed Directive is to provide throughout the Community for a basic level of protection of personal data and privacy for the European citizen, which should be included in the general new digital telecommunications offering, while referring requirements for enhanced levels of data security for specific individual cases and applications to the specific measures to be developed within the framework of the work plan set out in the Commission’s proposal for a Council Decision concerning security in information systems mentioned above.

The proposed Directive aims at achieving a basic level of protection of the general subscriber in the new digital environment by emphasising two fundamental principles:

- minimising the risk of abuse by limiting the data processed and stored in the context of public telecommunications operations to the bare minimum required for ensuring adequate operation, service quality and subscriber facilities;

- ensuring fully the right of the subscriber to information self-determination, both with regard to the telecommunications organisation providing the services as well as with regard to the second party in a call connection and any third party which may want to gain access to the data transmitted or provided in the context of a transaction via a public telecommunications network.

Given that the most profound impact on the general subscriber by the new telecommunications environment will be in the field of voice telephony, the proposed Directive concentrates on this area. However, it provides for a procedure for the application of the provisions relating to the voice telephone service to other public digital telecommunications services as applicable, such as for public data transmission services in the context of ISDN as well as public packet- and circuit-switched data networks, and other related public telecommunications services.

Further, given the current state of transition of the public telecommunications networks in the Community and in particular the fact that certain "Stored Programme-Controlled" (SPC) Exchanges, while not yet fully digital, do provide a number of the intelligent functions in question, the proposed Directive provides for those cases where a Member State has not yet implemented the Integrated Services Digital Network or public digital mobile networks, that the provisions of the Directive will be implemented to the extent that they also apply to services based on analogue networks.

With these general principles in mind, the content of the proposed Directive addresses in particular: the collection, storage and processing of personal data in the subscriber’s file; the storage and processing of traffic and billing data, in particular for the purpose of itemised call statements; the problem of the calling line identification; access by third parties; unsolicited calls; and the procedures to be chosen for establishing specific technical standards which may be required.

The articles of the Directive are briefly explained hereunder:

Articles 1 and 2 describe the overall objectives of the Directive and its
application to protection of data and privacy in connection with public telecommunications services in public digital telecommunications networks in the Community.

Article 3 contains definitions of important terms in line with the proposal of a Council Directive on the implementation of Open Network Provision (ONP) mentioned above.

The general principle in Article 4 that the collection, storage and processing of personal data by a telecommunications organisation is justified for the purposes of the provision of the intended service only and may not be used without specific permission by law or without the subscriber's prior recorded consent for any other purpose is applied in Article 5 to the establishment of subscriber files. As set out in the introductory statements to the Directive, such collection, storage and processing of personal data may in particular not be used to give telecommunications organisations any undue competitive advantage over other service providers in competitive fields.

Article 6 enumerates the rights of the subscriber concerning his personal data held by a telecommunications organisation and Article 7 states the principle of non-disclosure of such data to third parties without his consent or permission by law.

Article 8 should guarantee an adequate level of protection of data against unauthorised access.

Articles 9 and 10 apply the principle of collection, storage and processing of personal data as far as required for telecommunications purposes only to billing and traffic data. Article 11 intends to protect the privacy of the subscribers in connection with itemised call statements via the requirement of anonymity of the called subscriber.

Articles 12 and 13 contain detailed provisions concerning the calling line identification. The possibility to eliminate the identification feature should be made available, because, among other reasons, callers making calls to and from drug and alcohol rehabilitation centres, family abuse shelters or mental health services have a legitimate concern that this service feature may compromise their anonymity; the same applies to suicide and AIDS hot lines.

However, the called subscriber can have a legitimate interest in receiving only identified calls. In order to guarantee the right of information self-determination to both the calling and the called parties, the called subscriber must therefore have the possibility to limit the acceptance of incoming calls to those which identify the calling subscriber’s number.

Moreover, the telecommunications organisation should provide an override (blocking) function against the elimination of the identification feature in case of malicious calls; the function must also be made available for purposes of pursuit of criminal offences and for emergency services, in particular the fire brigade, in order to prevent abuse of such services.

Article 14 ensures that the privacy of both the calling and the called subscriber is also protected in case of the use of the call forwarding features.

---

13 See footnote 9.
Article 15 should prevent by technical means the contents of telephone calls being stored and/or disclosed to third parties without advance informing of the calling subscriber.

Articles 16 and 17 aim at preventing the unauthorized use of the subscribers' personal data by providers of teleshopping and videotex services in order to avoid the establishment of consumer profiles as well as at the protection of the subscriber's privacy against unsolicited messages, such as unwanted advertising via telecommunications means.

Article 18 is intended to prevent the fact that the introduction of technical features based on data protection requirements might create undue restrictions to the free circulation of telecommunications equipment and services in the Community, by ensuring, where required, the working out of common European standards for the implementation of specific technical features. In accordance with the Council Directive on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and telecommunications, the technical work is to be entrusted to the appropriate European standardisation bodies, in particular the European Telecommunications Standards Institute (ETSI) and the CEN/CENELEC.

The final provisions in articles 19 to 25 concern the field of application, the procedures for modifications necessary to adapt this Directive to new technical developments and consultation procedures. It is foreseen that a committee composed of representatives of the authorities responsible for data protection in the Member States and a committee composed of the representatives of the Member States shall assist the Commission in the implementation of the Directive. These committees are proposed to be the committees defined for these purposes in the draft Council Directive for the approximation of certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data submitted in parallel as mentioned above, but would be specifically constituted for the purposes of this Directive.

---


15 OJ NoL 36, 7 February 1987, p. 31.
IV. CONCLUSION

Effective Community-wide protection of personal data and privacy is developing into an essential pre-condition for social acceptance of the new digital networks and services.

Without a directive concerning the specific provisions necessary to implement the general principles of protection of personal data and privacy with regard to the specific requirements of public digital fixed and mobile networks, it will be impossible to prevent divergent developments in the Community which would very soon endanger the common market for both telecommunications services and terminal equipment.

The attached draft Directive is to provide for these specific provisions.

The Council is therefore requested to adopt the attached proposal for a Directive.
PROPOSAL FOR A COUNCIL DIRECTIVE CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF PUBLIC DIGITAL TELECOMMUNICATIONS NETWORKS, IN PARTICULAR THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND PUBLIC DIGITAL MOBILE NETWORKS
THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Article 100a thereof;

Having regard to the proposal from the Commission;

In co-operation with the European Parliament;

Having regard to the opinion of the Economic and Social Committee;

1. Whereas Council Directive concerning the protection of individuals in relation to the processing of personal data exorts Member States to ensure the protection of privacy;

2. Whereas currently in the European Community new advanced digital public telephone networks are emerging which give rise to specific requirements concerning the protection of personal data and privacy of the user;

3. Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and public digital mobile networks;

---

1...

2...

3...
4. Whereas the Council in its Resolution of 30th June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18th July 1989 on the strengthening of the co-ordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;

5. Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

6. Whereas Commission Recommendation 81/679/EEC calls for the adoption and ratification by Member States of the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data which spells out general principles for the protection of personal data;

7. Whereas a number of Member States have adopted and ratified this Convention;

8. Whereas Council Decision opens negotiations with a view to the accession of the European Economic Community, in the fields in which it is competent, to the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data.

5 OJ No C 196, 1.8.1989, p. 4.
7 OJ No C 12, 16.1.1989, p. 69.
8 OJ No C 12, 16.1.1989, p. 66.
9 OJ ...
9. Whereas Council Directive ..., concerning the protection of individuals in relation to the processing of personal data implements the adoption of these general principles in the Community.

10. Whereas in the case of public digital networks, specific legal, regulatory, and technical provisions must be made in order to protect personal data and the privacy of users with regard to the increasing risks connected with the computerized storage and processing of personal data in such networks;

11. Whereas Member States are currently developing divergent provisions in this area;

12. Whereas given the obstacles resulting from these divergent legal, regulatory, and technical provisions concerning the protection of personal data and privacy in the context of the implementation of public digital telecommunications networks in the Community, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks, the full establishment of a Community-wide market in telecommunications services and equipment requires the rapid introduction of harmonised provisions;

13. Whereas this Directive should determine the extent to which personal data may be collected, stored and processed in connection with the provision of telecommunications services;

14. Whereas the collection, storage, and processing of personal data by a telecommunications organisation is justified for the purposes of the provision of the intended service only and may not be used without specific authorization by law or the subscriber's prior consent for any other purpose; whereas such collection, storage, and processing of personal data may, in particular, not be used to give such telecommunications organisation any undue competitive advantage over other service providers;
15. Whereas this Directive should implement in the telecommunications sector the general principles concerning the subscriber's right to inspect the personal data stored about him/her, his right to request the rectification or erasure of such data, if necessary, as well as his right to prevent non-authorized disclosure of his personal data;

16. Whereas this Directive must provide for harmonization of the Member States' rules concerning the protection of privacy in the field of itemized call statements;

17. Whereas, it is necessary, as regards the calling line identification, to protect both the right of the calling party to remain anonymous and the privacy of the called party with regard to unidentified calls;

18. Whereas safeguards must be provided for the users of teleshopping and videotex services against unauthorized use of their personal data as well as for the subscribers in general against intrusion into their privacy by means of unsolicited calls;

19. Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market of 1992;

20. Whereas the implementation of this Directive with regard to third countries must take into account the level of protection of personal data and privacy in those countries as provided for in Council Directive concerning the protection of individuals in relation to the processing of personal data;

21. Whereas all matters concerning protection of personal data and privacy in the context of public digital telecommunications networks, which are not covered by the provisions of this specific Directive, the Council Directive mentioned above shall apply;

22. Whereas this Directive does not address issues of protection of personal data and privacy related to national security;
23. Whereas it is useful for the preparation of measures intended to implement or modify this Directive to draw on the experience of the Working Party on the Protection of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 27 of Council Directive ..., concerning the protection of individuals in relation to the processing of personal data.

24. Whereas such measures must be prepared with the assistance of the committee composed of representatives of the Member States set up by Article 30 of Council Directive ..., concerning the protection of individuals in relation to the processing of personal data.
HAS ADOPTED THIS DIRECTIVE:

Article 1

1. This Directive provides for the harmonisation of the provisions required to ensure an equal level of protection of privacy in the Community and to provide for the free movement of telecommunications equipment and services within and between Member States.

2. The Member States shall adopt the necessary specific provisions in order to guarantee the protection of personal data and privacy in the telecommunications sector in accordance with this Directive.

Article 2

1. Without prejudice to the general provisions of Council Directive ..., concerning the protection of individuals in relation to the processing of personal data, this Directive applies specifically to the collection, storage, and processing of personal data by telecommunications organizations in connection with the provision of public telecommunications services in public digital telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. In case a Member State has not yet implemented the Integrated Services Digital Network (ISDN) or public digital mobile networks, the provisions of this Directive will be implemented to the extent that they also apply to services based on analogue networks.
Article 3

For the purposes of this Directive,

1. "personal Data" means any information relating to an identified or identifiable individual;

2. "telecommunications organization" means a public or private body, to which a Member State grants special or exclusive rights for the provision of a public telecommunications network and, where applicable, public telecommunications services;

3. "public telecommunications network" means the public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means;

4. "public telecommunications service" means a telecommunications service whose supply Member States have specifically entrusted inter alia to one or more telecommunications organizations.

Article 4

1. Collection, storage and processing of personal data by a telecommunications organization is justified for telecommunications purposes only, in particular in order to establish connections for the transmission of voice, data or image, to produce bills, to compile directories, and for other legitimate operational purposes, for example fault clearance, prevention of misuse of the telecommunications organization's equipment, or registration of incoming calls in accordance with Article 13(1).

2. The telecommunications organization shall not use such data to set up electronic profiles of the subscribers or classifications of individual subscribers by category.
Article 5

1. Personal data of the subscriber may be collected and stored to the extent necessary to conclude, perform, amend or terminate the contract with the telecommunications organization. After termination of the contract the data are to be erased unless and for so long as they are required to deal with complaints, to recover charges or to comply with other obligations imposed by the law of the Member State, in conformity with Community law.

2. The contents of the information transmitted must not be stored by the telecommunications organization after the end of the transmission, except where required by obligations imposed by the law of the Member State, in conformity with Community law.

Article 6

The subscriber is entitled

- to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him/her are stored as well as communication to him/her of such data in an intelligible form,

- to obtain, as the case may be, rectification or erasure of such data if they have been processed in breach of the provisions which are imposed by the law of the Member State in conformity with Community law.
Article 7

1. In principle, all personal data processed in connection with telecommunication networks and services are to be kept confidential.

2. The personal data may not be disclosed outside the services or the network of the telecommunications organization without specific authorization by law or the subscriber's prior consent. A subscriber shall be held to have given such consent only where it is given by way of a specific response to a request by the telecommunications organization. Without the subscriber's prior consent, these personal data must not be disclosed to persons within the telecommunications organization who are not dealing with the relevant services provided.

3. The telecommunications organization must not make the provision of its service dependent upon such consent.

Article 8

1. The telecommunications organization must provide adequate, state-of-the-art protection of personal data against unauthorized access and use.

2. In case of particular risk of a breach of the security of the network, for example in the field of mobile radio telephony, the telecommunications organization must inform the subscribers concerning such risk and offer them an end-to-end encryption service.
Article 9

1. Billing data containing the telephone number or identification of the subscriber station, the address of the subscriber and the type of station, the total number of units to be charged for the accounting period, the called telephone number, the type and duration of the calls made and/or the data volume transmitted as well as other information needed for billing such as advance payment, payment by instalments, disconnection and reminders, may be stored and processed.

2. Such a general storage of billing data is permissible up to the end of the statutory period during which the bill may be challenged.

Article 10

1. Traffic data containing the personal data necessary to establish calls, or required for billing or other operational purposes, such as the telephone number of the calling and of the called subscriber, the time each call started and finished and the telecommunications service used by the subscriber, may be collected, stored and processed as far as this is necessary to provide the telecommunications service required.

2. The traffic data stored in the switching centres of the telecommunications organization must be erased after termination of the call unless the data are anonymised or are required for billing or other legitimate purposes in the meaning of Article 4.

Article 11

Upon application of the subscriber an itemized call statement may be produced, containing, among other items, the telephone numbers of the called subscribers without the last four digits.
Article 12

1. With regard to communications between subscribers linked to digital exchanges, the calling subscriber must have the possibility to eliminate via a simple technical facility the identification of his/her telephone number on the display of the called subscribers' terminal equipment, or its recording in a storage facility of this terminal, on a case-by-case basis.

   The transmission of the telephone number may also be permanently eliminated by the telecommunications organization upon application of the calling subscriber.

2. The called subscriber may apply for permanent elimination of the identification of all incoming calls; he/she must also be able to turn off the display of his/her terminal equipment, or to eliminate the recording in the terminal's storage facility, in order to prevent the identification of the incoming calls, on a case-by-case basis.

   The called subscriber must be able to limit the acceptance of incoming calls to those which identify the calling subscriber's number.

3. With regard to communications between a subscriber linked to an analogue exchange and subscribers linked to digital exchanges, the former subscriber is to be informed of the identification of his/her telephone number and to be offered the permanent elimination of the feature upon application. This subscriber must also have the possibility to eliminate the identification on a case-by-case basis.
Article 13

1. For a limited period of time, the telecommunications organization may override the elimination of the calling line identification

a) upon application of a subscriber requesting the tracing of malicious calls. In this case, the data containing the identification of the calling subscriber will be stored by the telecommunications organization and be made available upon request to the public authority charged with the prevention or pursuit of criminal offences of the Member State concerned;

b) upon specific court order, in order to prevent or pursue serious criminal offences.

2. A permanent override function must be made available upon request,

a) to organizations recognized by a Member State which answer and deal with emergency calls, and

b) to fire brigades operated or recognized by a Member State.

3. The telecommunications organisations shall take the necessary steps to ensure that the override function is operational on a national and Community-wide basis.

Article 14

1. Calls may be forwarded from the called subscriber to a third party only if this party has agreed; the third party may limit automatic forwarding to those calls which identify the calling subscriber's number; the third party must be informed via a specific signal of the message that the call has been forwarded.

2. The calling subscriber must be informed automatically during the establishment of the
connection that the call is being forwarded to a third party.

Article 15

1. If the content of telephone calls is made accessible to third parties via technical devices, such as loudspeakers or other on-hook equipment, or stored on tape for own use or use by third parties, provision must be made in order that the parties concerned are informed via an appropriate procedure of such diffusion or storage before the diffusion or storage is initiated and for so long as it continues.

2. Paragraph 1 does not apply in the cases covered by Article 13(1).

Article 16

1. The telecommunications organization must ensure that the telephone number as well as other personal data of the subscriber, in particular concerning the quantity and nature of his/her orders when using a teleshopping service or concerning the information requested via a videotex service, is stored only to the extent strictly necessary to supply the service and is only used by the service provider for purposes authorized by this subscriber.

2. Subject to the provisions of Article 20, the service provider may not set up electronic profiles of the subscribers or classifications of individual subscribers by category, without their prior consent.
Article 17

1. Subscribers who receive unsolicited calls for advertising purposes or for the purpose of offering the supply or provision of goods and services may notify the telecommunications organization conveying such messages that they do not wish to receive these calls.

2. The telecommunications organization must take the steps necessary to terminate the transmission of such messages to the subscribers concerned. Furthermore, the telecommunications organization must keep a list of the notifications in a form specified and available for inspection by the regulatory authority, in order to prevent such calls in future.

Article 18

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 can only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council Directive 83/189/EEC\(^\text{10}\) which lays down a procedure for the provision of information in the field of technical standards and regulations.

\(^\text{10}\) OJ No L 109, 26.4.1983, p.8.

Article 19

1. The provisions of this Directive relating to the telephone service shall be applied to other public digital telecommunications services to the extent that these services present similar risks for the privacy of the user.

2. The measures necessary for the implementation of paragraph 1 shall be adopted by the Commission after consultation of the working party referred to in Article 22 and in accordance with the procedure laid down in Article 23.

Article 20

To the extent that the full achievement of the objectives of this Directive requires the application of its provisions to service providers other than telecommunications organizations, the Commission may adopt the measures necessary for the application of this Directive to those service providers after consultation of the working party referred to in Article 22 and in accordance with the procedure laid down in Article 23.

11 OJ No L 36, 7.2.1987, p. 31.
12 OJ No L 36, 7.2.1987, p. 31.
Article 21

The details of the application of this Directive and the modifications necessary to adapt this Directive to new technical developments shall be determined by the Commission in accordance with the procedure laid down in Article 23.

Article 22

1. The Working Party on the Protection of Personal Data established according to Article 27 of Council Directive approximating certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data shall carry out the tasks laid down in Article 28 of the above mentioned Directive also with regard to the data protection measures which are the subject of this Directive.

2. The working party will be specifically constituted for the purposes of this Directive.

Article 23

1. The procedure laid down in Article 30 of Council Directive approximating certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data shall apply.

2. The committee established in the framework of that procedure will be constituted specifically for the purposes of this Directive.
Article 24

1. The Member States shall bring into force the laws, regulations, and administrative provisions necessary for them to comply with this Directive by 1 January 1993 at the latest.

The provisions adopted pursuant to the first subparagraph shall make express reference to this Directive.

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

Article 25

This Directive is addressed to the Member States.

Done at Brussels, For the Council
La protection des données à caractère personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, et en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics.

1. Ligne budgétaire concernée
   En 1990 : B 7700
   En 1991 et exercices ultérieurs : B5-4010

2. Base légale
   Article 100 A

3. Proposition de classification en dépense obligatoire / non obligatoire
   non-obligatoire

4. Description et justification de l'action :

   4.1. Objectifs :
      - assurer la protection des personnes à l'égard des données à caractère personnel,
      - permettre la circulation transfrontalière de données à caractère personnel dans la Communauté,
      - permettre le bon fonctionnement du marché intérieur.

   4.2. Réunions spécifiques du groupe de protection des données à caractère personnel (Art. 22) et du Comité consultatif (Art. 23), créés par la directive, représentant les États membres.
4.3. Un représentant de la Commission préside le groupe de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du groupe et du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions

(frais de participation des membres des 2 Comités)

5.2. Calcul : - Groupe de protection des données : (cf. fiche financière de la directive générale)

- Comité consultatif :

24 membres (gouvernementaux) x 3 réunions x 2 jours x 390 ECU/jour = 56.160 ECU *

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

CE-CP

1993 : 56.160 ECU
1994 : 56.160 
1995 : 56.160 
1996 : 56.160 
1997 : 36.160-

6.2. Part du financement communautaire dans le coût total : 100 %

* estimation
7. **Observations**

1. **Le groupe de protection des données à caractère personnel (Art. 22)**:

Il est institué ce groupe à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tous les États membres, présidé par un représentant de la Commission.

Ce groupe établit son règlement intérieur. Le secrétariat du groupe est assuré par les services de la Commission.

Missions de ce groupe : voir Art. 22

2. **Le Comité consultatif (Art. 23)**

Il est institué un Comité consultatif composé des représentants des États Membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.
EXPLANATORY MEMORANDUM:

1. The protection of individuals with regard to the processing of personal data is both an individual right and a necessary precondition for the development of international trade.

2. The processing of personal data is indispensable for international trade in goods and services and for closer collaboration between countries.

3. The Commission has forwarded to the Council a proposal for a Directive on providing individuals throughout the Community with a high level of protection with regard to the processing of personal data. This action should be supplemented by initiatives designed to guarantee individuals an equivalent level of protection with regard to the exchange of data between the Community and non-member countries.

4. A Convention for the protection of individuals with regard to automatic processing of personal data was concluded in the Council of Europe in 1981. The purpose of the Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him. This Convention also lays down that a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

5. In its Recommendation of 29 July 1981, the Commission invited Member States of the Community to ratify the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. This Recommendation also specifies that if all the Member States do not sign and ratify the Convention within a reasonable time, the Commission reserves the right to propose that the Council adopt an instrument on the basis of the EEC Treaty.

6. This Convention has not yet been ratified by all Member States of the Community. It is necessary and desirable for the Community to accede to this Convention in order to ensure the protection of personal data and the transborder exchange of such data with non-member countries, and to make the Convention more attractive to non-member countries wishing to exchange data as freely as possible with the Community.

1. The Convention (STE 108 of 28 January 1981) has been signed by the following Member States: Belgium, Greece, Ireland, Italy, the Netherlands and Portugal. It has been ratified by Denmark, France, the Federal Republic of Germany, Luxembourg, Spain and the United Kingdom.
7. It is thus proposed that the Commission recommend the Council to authorize the Commission to negotiate with the Council of Europe and the States that are party to the Convention for the protection of individuals with regard to automatic processing of personal data an additional protocol that will enable the European Communities to become party to this convention for the fields for which they are responsible.

8. The Commission will conduct these negotiations in consultation with the representatives of the Member States, in accordance with the directives annexed to this Communication or of such as may be forwarded to it by the Council.

9. The Member States of the Community, all of which are members of the Council of Europe, will fully support Community action during the negotiations for the accession of the European Community whenever this question arises within the Council of Europe.

Annex: Negotiating directives
NEGOTIATING DIRECTIVES

1. The purpose of the negotiations is to conclude an additional protocol to allow the Community to become a contracting party to the Convention for the fields for which it is responsible. The following principles shall be respected:

2. The European Community shall be represented within the Consultative Committee set up under Article 18 of the Convention by the Commission of the European Communities.

After the Commission has arranged coordination at Community level, the representative of the European Community shall be given a number of votes equal to the total number of votes held by the national delegations of the Member States of the Community that are party to the Convention in all questions relating to the processing of personal data in the fields which are the responsibility of the Community.

In all other questions, each national delegation shall have one vote.

3. In order to ensure that the additional protocol allowing the Community to become a contracting party to the Convention enters into force within a reasonable time, the Commission, supported by the Member States, will propose that an opting out procedure for its adoption be included in the text of the protocol.
PROPOSAL FOR A COUNCIL DECISION

IN THE FIELD OF

Information Security
**Executive Summary**

Information under its various forms increasingly contributes to individual, corporate and national wealth. The growth and performance of an estimated 2/3 of the economy relies on manufacturing or services heavily dependent on information technology, telecommunications and broadcasting, and therefore depends critically on the accuracy, security and "trustworthiness" of information. This is of as great importance and interest for individuals as for commerce, industry and public administrations. Correspondingly, the protection of information in all its aspects, here referred to as Information Security\(^1\), has become a central policy issue and a major concern world-wide.

Major changes have occurred during the last decades, but those ahead may be even greater. Desk-top supercomputers, Satellite Direct Broadcasting, Digital Mobile Radio, Integrated Broadband Communications and other new applications of technologies are under development and will provide the means for low-cost, mobile, high performance communication world-wide on an unprecedented scale. The advent of efficient global communication has placed greater emphasis on the need to provide adequate "protection" over levels of service availability, message integrity and privacy commensurate with the expected level of administrative or technical threat.

The subject is of great importance for socio-economic development of the European Community and the completion of the internal Market in 1992. A consistent approach at European level should create at the same time an increasing feeling of confidence vis-a-vis the use of new information technology and telecommunication services and help to avoid the formation of new barriers between the individual Member States and with other countries. Therefore, there is an urgent need to address requirements and options for action at Community level in close collaboration with sector actors and Member States. Any action must take into account both national and international commercial, legal and technical developments. Because Information Security is involved in the protection not just of property and people, but also of society itself, Member States regard it as a topic which touches upon national sovereignty.

At the same time, for the Community and its Member States, it is vital that Information Security does not become a constraint to the promotion of harmonious development in the Community and to relations with other countries. As such, development of a harmonised approach to information security must form an integral part of the Community policies related to the strengthening of the European Community socio-economic performances, international competitiveness and the completion of the internal market.

The key issue is to provide effective and practical security for information held in an electronic form to the general users, administrations and the business community without compromising the interests of the public at large.

\(^1\) Information Security (IS) is concerned with the protection of information stored, processed or transmitted in electronic form, against deliberate and accidental threats. Electronic Information services need a secure telecommunication infrastructure, secure terminals (including processors and data bases) as well as secure usage.
Action at Community level will need to involve concerted efforts in establishing the required technology, standards, verification and certification procedures and regulations (where required) in the framework of the Community policy making.

The intention of the Commission is to encourage a debate with the sector actors in the Community on Information Security issues and to develop a consensus on the appropriate steps to be considered. This debate could be initiated on the basis of the statement of issues and lines of action identified in the annex to this note. In this debate, and in view of the responsibilities of Member States in this domain, it is of crucial importance that the Community initiative can rely on a close collaboration with senior officials of Member States.

It is therefore proposed that the Commission shall be assisted by a committee of an advisory nature, composed of representatives of the Member States and chaired by the representative of the Commission. The working of this committee has to reflect the specificities of the domain. This committee would be called the Senior Officials Group on Information Security (SOG-IS).

The most important issue of protection of personal data is dealt with in a proposal of Directive which is sent in parallel with the present communication.
A. New challenges and the Social, Economic, Strategic and Political Importance of Information Security

1. The management and use of information supported by Information Technology and Informatics Services in all spheres of economic, social and political life is pervasive. It has permitted the integration of activities via a global communications system, connecting manufacturing plants, research establishments, data bases, computer centres, service providers as well as centres of political and economic decision-taking.

2. This increased integration of separate activities generates very considerable value-added in terms of savings or increasing efficiency. It is therefore a key-factor in international competitiveness. However, it also increases the need to protect the justifiable interests of the individuals, the general public, commerce, industry, operators, services providers and national administrations.

3. For the service sector to grow, and with it investments in electronic equipment, telecommunications, broadcasting, computer and terminal equipment and a wide range of telematics applications to take place, a secure European Electronic Information Environment must be offered. Widespread acceptance and approval by all parties is important to safeguard legitimate interests and to prevent misuse and abuse of information. This must be achieved in a way which is both efficient yet adequate for users under various legal systems. In addition, information security systems must protect privacy, intellectual property, fair competition, national security and other interests.

4. With the introduction of microcomputers, the use of Information Technology, Telecommunications and Broadcasting has grown beyond the professional domain and has become a "consumer activity" with associated "consumer services". Along with this quantitative change, a very significant qualitative change has occurred: telecommunications now permits interworking and communication on a global scale.

5. Major changes have occurred during the last decades, but those ahead may be even greater. Desk-top supercomputers, Satellite Direct Broadcasting, Digital Mobile Radio, Integrated Broadband Communications and other new applications of technologies are under development and will provide the means for low-cost, mobile, high performance communication world-wide on an unprecedented scale.

6. The advent of efficient global communication represents a qualitatively and quantitatively new challenge for the need to provide adequate "protection" over levels of service availability, message integrity and privacy, commensurate with the expected level of administrative or technical threat.

7. The growing willingness of industry, government and society as a whole to use information services has resulted in them becoming an integral part to the basic fabric of every day life. Command, Communication and Control in general, Process Control in manufacturing, Transportation, Financial Services, Automated Office systems, etc all require levels of availability and operational robustness not fully understood in the original service or component design.

8. New applications will be defined and implemented that may not be achieved within the present architectural frameworks. A fundamental re-definition of architecture and performance standards (including the needs to assure conformance) relating to services and underlying components may be necessary.
9. New disciplines and supporting organisations/occupations will need to be created to achieve these higher levels of operational expectations. The major needs will, however, be driven by cultural not technical changes. The global exploitation of information services supported by comprehensive telecommunications networks will change the perception in society of organisational/human relationships.

10. Increasingly communication will either be through intermediaries, as in various levels of added-value services supported by IT, or will take place directly after intermediaries have approved the contact. In such situations trust will need to be explicitly defined in the context of organisational relationships, authorities/privileges and many service/product 'quality controls'. Care must be taken in such a society that the rights of individuals and organisations are fully reflected in legislation and regulatory controls. In parallel, technologies must be conceived and implemented in a way which meets security demands.

B. The need for an action at Community level in collaboration with Member States

11. With the protection of property, the person, and even society at stake, it is obvious that information security is an area of major responsibility for the Member States. Both for defense and the normal functioning of its institutions, each Member State is directly concerned with security. These national concerns of governments have led, historically, to a strong long-standing competence in information security, and the exercise of control over its technology and techniques to prevent the diffusion of sensitive aspects. Although each user must be responsible for choosing his own security, his choices rely essentially on guarantees which, in the final analysis, come from public authorities, through, for example the legal limits they fix.

12. EEC policies and programmes for the development of the Information and Telecommunication Industries and for the achievement of the Internal Market, may be seriously impeded unless an active policy is adopted on the initiation, development and promotion of Information Service Security Standards. For the Community, it is vital that Information Security does not become a constraint to the promotion of harmonious development within the Community and to relations with other countries. As such, development of a harmonised approach to information security must form an integral part of the Community policies related to the strengthening of the European industry socio-economic performance and international competitiveness, and to the completion of the Internal Market.

13. More specifically, it must involve concerted efforts in establishing the required standards, verification and certification procedures, technological developments and regulations (where required) in the framework of the Community policy making. Because of the highly technical nature of the underlying issues, concertation of efforts implies collaboration of actors at the pre-competitive stage of R&D

14. "Open Standards" adoption by Governments (US/UK GOSIP), by the western Defense community (NATO/NOSI), by the computer and telecommunications industry as well as network operators (ISO OSI standards) has resulted in greater emphasis on security issues in information systems, architectures, standards, communications protocols and component techniques.
15. Only an estimated 2% of the services which will be available in the Community by the year 2000 are available today. By then services will typically be able to respond to user needs and offer a range of integrated features combining voice, data and image in a flexible manner. The realisation of user requirements for information security such as data protection, privacy, authentication, authorisation, billing, etc. will correspondingly be much more difficult to assure. It is for this reason that Information Security and the related technical features such as integrity need to be systematically developed and investigated. US Authorities are funding programmes on Trusted Computer Systems, Open Systems Architectures, protocols and techniques that will accelerate the use of proprietary security solutions in the international user community. It must be a primary concern for Member States to be an equal partner in addressing standardisation in this domain. Following a de facto standardisation would risk creating new technological dependencies which may seriously impede the international competitiveness of Community's economies. This implies that the corresponding efforts are made in the Community as a prerequisite for a constructive interaction with countries outside the Community, mainly the US.

16. To sum it up, because of their respective responsibilities, both the Community and its Member States have a strong interest in the key questions:

- How will effective specifications and standards for information security be defined and promulgated?
- How will the formal evaluation and certification that products and systems conform to the security standards (both functionally and in giving assurance) be implemented?
- How will security products and systems be implemented, provided and used?

17. Information security is a typical example of a policy where the principle of subsidiarity may be applied, in view of the inherent complexity of the subject, the involvement of numerous actors and the necessity to deploy a range of policy tools. An action plan is essential telling what should be done, by whom and how. On the one hand, the Member States have to handle these questions; on the other hand, the Community has a strong interest in working out terms ensuring the compatibility between on one side the completion of the Internal Market, the achievement of the Citizens' Europe, the implementation of a telecommunications policy and the competitiveness of the European community electronics and electronic information services industries, and on the other side the response to the basic requirements of the individuals and the business for information security. Therefore, and in order to focus the effort, various types of actions and a procedural structure are proposed below as a basis for further in-depth studies leading to measures to be taken at the appropriate level.
Proposal for a
COUNCIL DECISION
IN THE FIELD OF
INFORMATION SECURITY

THE COUNCIL OF THE EUROPEAN COMMUNITIES

Having regard to the Treaty establishing the European Economic Community, and in particular Article 235 thereof,

Having regard to the proposal from the Commission,(1)

Having regard to opinion of the European Parliament,(2)

Having regard to the opinion of the Economic and Social Committee,(3)

Whereas the Community has as its task, by establishing a common market and progressively approximating the economic policies of the Member States, to promote throughout the Community a harmonious development of economic activity, a continued and balanced expansion, increased stability, accelerated raising of the standard of living, and closer relations of the States belonging to it;

Whereas information stored, processed and transmitted electronically plays an increasingly important role in social and economic activities;

Whereas the advent of efficient global communication and the pervasive use of electronic handling of information emphasises the need for adequate protection;

Whereas the European Parliament has repeatedly stressed the importance of information security in its deliberations and decisions;

(1) OJ No C...
(2) OJ No C...
(3) OJ No C...
Whereas the Economic and Social Committee has emphasised the need to address information security related issues in Community actions, particularly in view of the impact of the completion of the internal market;

Whereas it is necessary to develop a global strategy for information security in order to ensure the security of the user on the Community level and avoid the creation of new technical obstacles to communication;

Whereas the inherent complexity of information security issues calls for subsidiarity, the active involvement of several sectors and the concerted use of several policies;

Whereas actions on national, international and Community level provide a good basis;

Whereas there is a close link between telecommunications, standardisation, information market and RD&T policies and the work already undertaken in these domains by the European Community;

Whereas it is appropriate to assure the concertation of efforts, by building on existing national and international work and by promoting the cooperation of the principal protagonists concerned; whereas it is therefore appropriate to proceed within the framework of a coherent action plan;

Whereas the responsibility of the Member States in this domain implies a concerted approach based on a close collaboration with senior officials of the Member States.

HAS DECIDED AS FOLLOWS:

Article 1

1. An action plan in the field of information security (INFOSEC) is adopted for a period of 24 months starting on [ ].

2. The action plan is designed to develop a global strategy providing the users of electronically stored, processed or transmitted information with protection of information systems against accidental or deliberate threats.

3. The action will take into account and support the evolving European and world-wide standardisation activities in the field.
Article 2

The action plan, the details of which are set out in the Annex hereto shall comprise the following lines of action:

I. development of an information security strategy framework;
II. analysis of information security requirements;
III. solutions for immediate and interim needs;
IV. specifications, standardisation and verification of information security;
V. integration of technological and operational developments for information security within a general strategy;
VI. integration of certain security functions in information systems.

Article 3

The action plan shall be implemented by the Commission in collaboration with the organisations and enterprises concerned and in close association with the Member States.

Article 4

The amount attributed to this action shall be determined in the course of the annual budgetary procedure.

Article 5

The Commission shall send to the European Parliament and the Council a report on the results of the action within three months of its completion.

Article 6

For the implementation of the action plan, the Commission shall consult, as necessary, a Senior Officials Group on Information Security (SOGIS). This group shall consist of two representatives of each Member State and of the Commission. A Commission representative shall be in the chair.
The members of the Group may be assisted by experts or advisers depending on the nature of the issues under consideration.

The proceedings of the Group shall be confidential. The Group shall adopt its own rules of procedure. The secretariat shall be provided by the Commission.

Done at Brussels, For the Council
ANNEX

Summary of Action Lines


1.1 Issue

1. Information security is recognised as a pervasive quality necessary in modern society. Electronic Information services need a secure telecommunication infrastructure, secure terminals (including processors and data bases) as well as secure usage. An overall strategy, considering all aspects of information security, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.

1.2 Objective

2. A strategically oriented framework has to be established to reconcile social, economic and political objectives with technical, operational and legislative options. The sensitive balance between different concerns, objectives and constraints has to be found by sector actors working together in the development of a common perception and agreed strategy. These are the prerequisites for reconciling interests and needs both in policy making and in industrial developments.

1.3 Status and trends

3. The situation is characterized by growing awareness of the need to act. However, in the absence of an initiative to concert the efforts it seems very likely that dispersed efforts in various sectors will be taken which create de facto a situation which will be contradictory, creating progressively more serious legal, social and economic problems.

1.4 Requirements, options and priorities

4. Such a shared framework would need to address and situate risk analysis and risk management concerning the vulnerabilities of information and related services, the alignment of laws and regulations associated with computer/telecommunications abuse and misuse, administrative infrastructures including Security Policies and how these may be effectively implemented by various industries/disciplines, and social and privacy concerns (eg the application of identification, authentication and possibly authorization schemes in a democratic environment).

5. Clear guidance is to be provided for the development of physical and logical architectures for secure distributed information services, standards, guide-lines and definitions for assured security products and services, pilots and prototypes to establish the viability of various administrative structures, architectures and standards related to the needs of specific sectors.
6. Security Awareness must be created in order to influence the attitude of the users towards an increased concern about security in IT and telecommunication systems.


2.1 Issue

7. Information security is the inherent pre-requisite for the protection of privacy, intellectual property, commercial confidentiality and national security. This leads inevitably to a difficult balance and sometimes choices, between a commitment to free trade and a commitment to securing privacy and intellectual property. These choices and compromises need to be based on a full appreciation of requirements and the impact of possible information security options to respond to them.

8. User requirements imply information security functionalities interdependent with technological, operational and regulatory aspects. Therefore, a systematic investigation of information security requirements forms an essential part of the development of appropriate and effective measures.

2.2 Objective

9. Establishing the nature and characteristics of user requirements and their relation to information security measures.

2.3 Status and Trends

10. Up to now, no concerted effort has been undertaken to identify the rapidly evolving and changing requirements of the major actors for Information Security. EC Member States have identified the requirements for harmonisation of national activities (especially of the "IT security criteria"). Uniform evaluation criteria and rules for mutual recognition of evaluation results/certificates are of major importance.

2.4 Requirements, options and priorities

11. As a basis for a consistent and transparent treatment of the justified needs of the sector actors it is considered necessary to develop an agreed classification of user requirements and its relation to information security provision.

12. It is also considered important to identify requirements for legislation, regulations and codes of practice in the light of an assessment of trends in service characteristics and technology, to identify alternative strategies for meeting the objectives by administrative, service, operational and technical provisions, and to assess the effectiveness, user-friendliness and costs of alternative information security option and strategies for users, service providers and operators.
3. Action Line III - Solutions for Immediate and Interim Needs

3.1 Issue

13. At present it is possible to protect adequately computers from unauthorised access from the outside world by "isolation" ie by applying conventional organisational and physical measures. This applies also to electronic communications within a closed user group operating on a dedicated network. The situation is very different if the information is shared between user groups or exchanged via a public, or generally accessible, network. Neither the technology, terminals and services nor the related standards and procedures are generally available to provide comparable information security in these cases.

3.2 Objective

14. The objective has to be to provide, at short notice, solutions which can respond to the most urgent needs of users. These should be conceived as open towards future requirements and solutions.

3.3 Status and trends

15. Some user groups have developed techniques and procedures for their specific use responding, in particular, to the need for authentication, integrity, and non-repudiation. In general magnetic cards or smart cards are being used. Some are using more or less sophisticated cryptographic techniques. Often this implied the definition of user-group specific "authorities". However, it is difficult to generalise these techniques and methods to meet the needs of an open environment.

16. ISO is working on OSI information security (ISO DIS 7498-2) and CCITT in the context of X400. It is also possible to insert information security segments into the messages. Authentication, integrity and non-repudiation are being addressed as part of the messages (EDIFACT) as well as part of the X400 MHS.

17. Presently, the EDI legal framework is still at the stage of conception. The International Chamber of Commerce has published uniform rules of conduct for the exchange of commercial data via telecommunications networks.

18. Several countries (eg FRG, France, the UK and US) have developed or are developing criteria to evaluate the trustworthiness of IT and telecommunication products and systems and the corresponding procedures for conducting evaluations. These criteria have been coordinated with the national manufacturers and will lead to an increasing number of trusted products and systems starting with simple products. The establishment of national organisations who will conduct evaluations and offer certificates will support this trend.

19. Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services and in particular mobile services will have become all pervasive.

3.4 Requirements, options and priorities

20. It is essential to develop as soon as possible the procedures, standards, products, and tools suited to assure information security on public communications networks. A high priority should be given to authentication, integrity and non-repudiation. Pilot projects should be carried out to establish the validity of the proposed solutions. Solutions to priority needs on EDI are looked at in the TEDIS programme within the more general content of this action plan.

4.1 Issue

21. Information security requirements are pervasive and as such common specifications and standards are crucial. The absence of agreed standards and specifications may present a major barrier to the advance of information-based processes and services throughout the economy and society. Actions are required to accelerate the development and use of technology and standards in several related communication and computer network areas that are of critical importance to users, industry and administrations.

4.2 Objective

22. Efforts are required to provide a means of supporting and performing specific functions in the general areas of OSI, ONP, ISDN/IBC, network management and network security for unclassified, but sensitive, information. Inherently related to standardisation and specification are the techniques and approaches required for verification.

4.3 Status and trends

23. The US, in particular, have taken major initiatives to address information security in the non-defence domain. In Europe the subject is treated in the context of IT and Telecommunications standardisation in the context of ETSI and CEN/CENELEC in preparation of CCITT and ISO work in the domain.

24. In view of growing concern, the work in the US is rapidly intensifying and both vendors and service provider are increasing their efforts in this domain. In Europe, France, the Federal Republic of Germany and the United Kingdom have independently started similar activities but a common effort corresponding to the US is only evolving slowly.

4.4 Requirements, options and priorities

25. In information security there is inherently a very close relationship between regulatory, operational, administrative-and technical aspects. Regulations need to be reflected in standards and information security provisions need to comply in a verifiable manner to the standards and regulations. In several aspects regulations require specifications which go beyond the conventional scope of standardisation, ie include codes of practice. Requirements for standards and codes of practice are present in all areas of Information Security, and a distinction has to be made between the protection requirements which correspond to the security objectives and some of the technical requirements which can be entrusted to the competent European standard bodies (CEN/CENELEC/ETSI).

26. Specifications and standards must cover the subjects of Information Security Services (personal and enterprise authentication, non-repudiation protocols, legally acceptable electronic proof, authorisation control), Communication Services (image communication privacy, mobile communications voice and data privacy, data and image data-base protection, integrated services security), Communication and Security Management (public/private key system for open network operation, network management protection, service provider protection) and Certification (information security assurance criteria and levels, security assurance procedures).
5. Action Line V - Technological and Operational Developments for Information Security

5.1 Issue

27. Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future information security requirements is a prerequisite to the development of the services market and the competitiveness of the European economy as a whole.

28. Any technological developments in information systems security will have to include both the aspects of computer security and security of communications as most present-day systems are distributed systems, and access to such systems is through communications services.

5.2 Objective

29. Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future information security requirements.

5.3 Requirements, options and priorities

30. Work on information security would need to address development and implementation strategies, technologies, and integration and verification.

31. The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise), functional requirements models, risk models, and architectures for security.

32. The technology orientated R&D work would have to include user and message authentication (e.g., through voice analysis and electronic signatures), technical interfaces and protocols for encryption, access control mechanisms, and implementation methods for provable secure systems.

33. Verification and validation of technical system security and its applicability would be investigated through integration and verification projects.

34. In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

35. The 3rd RDT Community Framework Programme might be used to foster cooperative projects at precompetitive and prenormative levels.

6.1 Issue

36. Depending on the exact nature of the Information security features required functions will need to be incorporated at different parts of the communication systems including terminals/computers, services, network management to cryptographic devices, smart cards, public and private keys etc. Some of these can be expected to be embedded in the hardware or software provided by vendors while others may be part of distributed systems (eg network management), in the possession of the individual user (eg smart cards) or provided from a specialised organisation (eg public/private keys).

37. Most of the information security products and services can be expected to be provided by vendors, service providers or operators. For specific functions, eg the provision of public/private keys, auditing, authorisation there may be the need to identify and mandate appropriate organisations.

38. The same applies for certification, evaluation and verification of quality of service which are functions which need to be addressed by organisations independent of the interests of vendors, services providers or operators. These organisations could be private, governmental, or licensed by government to perform delegated functions.

6.2 Objective

39. In order to facilitate a harmonious development of the provision of information security in the Community for the protection of the public and of business interests it will be necessary to develop a consistent approach as to the provision of information security. Where independent organisations will have to be mandated, their functions and conditions will need to be defined and agreed and where required embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

6.3 Status and trends

40. At present information security provision is well organised only for specific areas and limited to addressing the specific needs. The organisation on a European level is mostly informal and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of information security the need for defining a consistent approach to information security provision in Europe and internationally is becoming urgent.

6.4 Requirements, options and priorities

41. Because of the number of different actors concerned and the close relations to regulatory and legislative questions it is particularly important to pre-agree on the principles which should govern the provision of information security.

In developing a consistent approach to this question one will need to address the aspects of identification and specification of functions requiring, by their very nature, the availability of some independent organisation, (or interworking organisations). This could include functions such as the administration of a public/private key system;
In addition, it is required to identify and specify, at an early stage, the functions which
in the public interest need to be entrusted to independent organisation (or interworking
organisations). This could, for example include auditing, quality assurance, verification,
certification and similar functions;
BUDGET HEADING
Subsection B6, Item 8104

2. LEGAL BASE AND PROPOSED CLASSIFICATION
Article [235]
Non compulsory expenditure.

3. DESCRIPTION
Collaboration in the development of proposals and actions relating to information security as far as they require or significantly benefit from a concerted approach at Community level. The focus of the work is to relate to the needs of the general public, commerce, service providers and administrations and addresses the requirements for a collaborating approach to technological research, standardisation and related issues as relevant for the development or a consistent European approach to information security with particular reference to the completion of the internal market in 1992.

The goal of the INFOSEC action is to make a major contribution to the objective of the

"development of actions to providing effective and practical security for information held in an electronic form to the general users, administrations and business community without compromising the interest of the public at large."

The present proposal is the result of the preliminary investigations by experts, consultations and on-going related work.

The scope of the preparatory action is to focus on

I. development of an information security strategy framework
II. information security requirements
III. solutions for immediate and interim needs
IV. specifications, standardisation and verification of information security
V. technological and operational developments for information security
VI. information security provision.
4. JUSTIFICATION

Development of a harmonised approach to information security must form an integral part of the Community policies related to the completion of the Internal Market, strengthening of socio-economic performance and international competitiveness. It is vital that Information Security does not become a constraint to the promotion of harmonious development in the Community and to relations with other countries. In addition, information security systems must protect privacy, intellectual property, fair competition, national security and other interests.

The proposed action responds to an urgent need to facilitate and accelerate the emergence of generally accepted, effective and practicable measures on information security. The action will benefit from synergies with on-going programmes in the field of information technologies (ESPRIT) and telecommunications (RACE) as well as the on-going work on telecommunications, standardisation and information market policies.

5. INDICATIVE FINANCIAL PLANNING

5.0 Implications for expenditure.

5.0.0 Total cost over the whole of the expected duration of 2 years (in MioECU):

<table>
<thead>
<tr>
<th>From the Budget of the Communities:</th>
<th>12.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the other sectors at the national level:</td>
<td>0.0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>12.0</strong></td>
</tr>
</tbody>
</table>

5.0.1 Multi-annual schedule (in MioECU):

<table>
<thead>
<tr>
<th>Commitment Appropriations</th>
<th>Payment Appropriations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1991</td>
<td>2</td>
</tr>
<tr>
<td>1992</td>
<td>6</td>
</tr>
<tr>
<td>1993</td>
<td>2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>12</strong></td>
</tr>
</tbody>
</table>

5.0.2 Method of calculation

a) Expenditure by contract

This expenditure covers the Community's financial contribution to analytical work as required to support the development of specific actions proposed, reconsultation and establishment of consensus.
b) Operational expenditure

Given the fact that the action is financed in Subsection 6 of the budget devoted to Research and Investment expenditure, administrative costs (Committee and working party meetings, consultation of experts, missions, document distribution or dissemination of techniques, use of data processing, telecommunication and broadcasting equipment) are covered directly by the budget item.

The following table gives the indicative breakdown over the various categories of expenditure (in MioECU):

<table>
<thead>
<tr>
<th>S.0.2</th>
<th>1991</th>
<th>1992</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>4,823</td>
<td>4,100</td>
</tr>
<tr>
<td>b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in total</td>
<td>1,177</td>
<td>1,900</td>
</tr>
<tr>
<td>of which</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experts</td>
<td>0.400</td>
<td>0.600</td>
</tr>
<tr>
<td>Other operational expenditure</td>
<td>0.500</td>
<td>0.725</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>0.030</td>
<td>0.100</td>
</tr>
<tr>
<td>Information and publication</td>
<td>0.050</td>
<td>0.100</td>
</tr>
<tr>
<td>Statutory staff</td>
<td>0.177</td>
<td>0.375</td>
</tr>
</tbody>
</table>

6. FINANCIAL IMPLICATIONS FOR STAFF AND CURRENT ADMINISTRATIVE APPROPRIATIONS

The statutory research staff involved, i.e. 3 A, 1·B, 1·C, will be entered in the research staff table and is paid out of the appropriations entered onto Item B6-8104.

The administrative expenditure will be governed by the internal rules on mini-budgets decided by the Commission on 22 May 1990.

FINANCING OF EXPENDITURE

The appropriations to cover the Community's contribution to this project will be determined in the context of the annual budgetary procedure.

e. IMPLICATIONS FOR REVENUE

Contribution of the statutory research staff to the retirement scheme and the sickness insurance.
9. **TYPE OF CONTROL**

- Administrative control by the Director General for Financial Control as regards budget implementation;

- Control of achievement:  
  - SOG-IS  
  - control by officials of the Commission  
  - audit by the Court of Auditors in accordance with provisions of the Treaty;

- In accordance with Article 2 of the Financial Regulations, the use of appropriations will be subject to analyses of cost-effectiveness and the realisation of quantified objectives will be monitored.
OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Telecommunications)
on: 5 October 1990

No. Com prop.: 8460/90 ECO 158 COM(90) 314 final SYN 287-288

Subject: Protection of individuals in relation to the processing of personal data in the Community and information security

At its meeting on 5 October, the Working Party held an initial discussion on that part of the above communication specific to telecommunications, taking the form of a proposal for a Council Directive concerning the protection of personal data in the context of public digital telecommunications networks.

The discussion centred mainly on the method to be followed for examining the proposal.
It emerged from the discussion that:

- in most delegations' view, the Working Party could not examine the measures specific to telecommunications effectively unless this was done in close liaison with the proceedings to take place on the communication's key Directive in another Council Working Party (1);

- however, some delegations considered that the Working Party could nevertheless make a start on examining the telecommunication's proposal without excessive delay in order to identify those technical aspects of that proposal which came mainly within the telecommunications field.

(1) According to information received from the Secretariat of the Working Party which is to examine the key Directive, work on it is planned to start later this year.
OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Data Protection)
on: 25 February 1991

N° prop. Cion: 8460/90 ECO 158 - COM(90) 314 final - SYN 287-288

Subject: Protection of individuals in relation to the processing of personal data in the Community and information security


I. Introductory remarks by the Chairman

2. The Chairman of the Working Party congratulated the Commission for its initiative and its courage to have submitted in September 1990 the file on personal data protection. This file, which had been elaborated with great professional conscientiousness, constituted, in the Chairman's view, an excellent basis for the Working Party's discussion.
Although appreciating the initiative by the Commission, the Chairman did however regret that this initiative had only been taken at the end of 1990. He recalled that already in 1976 the European Parliament had adopted resolutions on the subject and that already in 1981 the Commission in a recommendation had stressed the fundamental right character of personal data protection.

Taking into account that the internal market should be operational by 1 January 1993 and taking into consideration also that the absence of a Community protection system would constitute an obstacle to the creation of an internal market, the Working Party found itself under serious time pressure. Only with the active collaboration of all delegations would it be possible for the Working Party to complete its work in time for Council adoption before the end of 1992.

II. Introductory remarks by the Representative of the Commission

3. Having thanked the Presidency for according a high priority to the Commission's proposal concerning the protection of personal data, the Representative of the Commission stressed the great importance of the issue for Community citizens, administrations, research bodies and industry. From discussions with representatives from all possible interests, including national supervisory authorities, academic institutions, professional associations and a large number of industries, a clear consensus that Community action in this field was necessary had emerged.

4. Outlining the developments and motives which led the Commission to take the initiative, the Representative of the Commission recalled that already in the 1970s, when the
first data protection laws appeared in Europe and the European Parliament issued its first two resolutions on this matter, it had become quite clear that this was not exclusively a human rights issue but an issue which also had important economic and strategic dimensions. This had been stressed in both international initiatives that appeared at the time, i.e. the Council of Europe Convention n° 108 and the OECD Privacy Guidelines. It had furthermore been stressed by the Commission when in July 1981 it issued a recommendation urging Member States to ratify Convention 108 at the same time stating that if all the Member States did not within a reasonable time sign and ratify the Convention the Commission reserved the right to propose that the Council adopt an instrument on the basis of the EEC Treaty.

If in 1981 economic side-effects from lack of harmonization had been feared, mostly in the field of computer and data processing services, today, ten years later, insufficient harmonization of Member States legislation directly affected the whole process leading to the single market and a citizens’ Europe. Free exchange of information was necessary between companies in the context of commercial and industrial activities, between research institutions, but also between administrations, including customs, police and social security authorities. At the same time information and data were becoming increasingly easy to manipulate. This fact plus the growing flow of information throughout the Community made the question of adequate protection of personal data a very pressing one.

Free exchange of information, and in particular personal information, would be very difficult without an adequate level of personal data protection throughout the Community. This had already been witnessed in the context of the Schengen agreement and in the context of bilateral
cases including cases between Community Member States and between countries parties to the Council of Europe Convention. Moreover, strong divergences among national laws carried the risk of creating market distortions in favour of the countries with the most lenient or least effective laws.

The main objectives of the Commission's proposal were therefore:

- to establish an adequate level of protection throughout the Community;

- to prevent barriers to information flows within the Community on data protection grounds;

- to establish certain specific procedures aiming at approximating to some extent national laws;

- to ensure that Community citizens' data were not abused outside the Community and Community data protection law was not circumvented through operations in third countries; and

- to establish mechanisms and procedures for additional initiatives including sectoral codes of practice and Community instruments, further national law approximation steps and if necessary amendments to the directive itself.

As regards the reactions received including a very large number of detailed written comments from industry associations and data protection authorities, the Representative of the Commission indicated that there had not been a single case of objections to the principles of data protection and the need for Community action. Starting
from this consensus, comments had gone in the direction of both more and less strict provisions. In some cases they showed a simple misunderstanding of the Commission’s text or intentions, while in some other cases they went further and questioned basic issues including the scope, the definitions, the respective treatment of the public and the private sectors, the question of transborder data flows, etc.

The Representative of the Commission went on to stress that the Commission had taken into account the fact that relevant laws exist already in 7 Member States. It had tried to take up those national law elements that it considered most appropriate. It had however had to introduce certain novelties, notably those concerning export of data to third countries, applicable law in transborder flow cases and mechanisms for further Community cooperation and action.

III. General reactions from delegations to the proposal by the Commission

5. The Italian delegation congratulated the Commission for the work it had done which in its view constituted an excellent starting point for the discussions of the Working Party. The Italian delegation did not however wish to give a detailed reaction to the Commission’s proposal, as the proposal was still under examination by the Italian authorities and this especially in respect of the ramifications with regard to the Council of Europe Convention and the Schengen agreement. The examination being carried out by the Italian authorities also included the question of the legal basis of the proposal.
6. The Irish delegation informed the Working Party that Ireland, two years ago, had enacted legislation to give effect to the Council of Europe Convention on data protection. In doing so Ireland had wished to strike a balance between the rights of individuals and the concern of not overburdening industry and the public sector. The legislation, which could be described as a second generation data protection law, had proved to be effective and only few complaints to the supervisory authorities had been made.

7. As regards specifically the proposal by the Commission, the Irish delegation indicated that very strong opposition had been voiced by public departments in Ireland and this mainly for the following reasons:

- the main justification for the proposed Directive was that ratification by all the Member States of the European Communities of the Council of Europe Convention would not provide an adequate solution as a fair level of appreciation was left to the States parties to the Convention with the result that the level of protection would vary between the Member States and thus prevent the free flow of data between Member States of the EC. Although the Directive tried to avoid this by giving extremely detailed rules, it did however also leave a certain amount of discretion to the Member States and this was indeed anticipated in Article 28; there therefore seemed to be a contradiction between the justification for the Directive and its actual contents;

- it had to be recognised that in the different States having legislation in the field of data protection there were different data protection cultures based on the existence of different legal concepts and different social environments and that in spite of this each
system operated satisfactorily. The concepts of the Directive were either unknown in some States or would be understood differently in the different Member States, prejudicing even further the aim of achieving equivalent protection in all Member States:

- the fears expressed in respect of the safeguard of the right of privacy had arisen especially in relation to the evolution in respect of personal data which had undergone automatic processing which permitted the storage of an enormous amount of data - these fears did not exist to the same extent in relation to manual files and the inclusion of such files within the scope of the directive was therefore not necessary and would only create an unnecessary administrative burden in a climate becoming increasingly competitive.

8. Because of the kind of problems raised by the Irish delegation, this delegation felt that it would be difficult to establish Community legislation to be enacted before the end of 1992. On a personal basis the representative of Ireland indicated that he preferred the following two-tier system:

- in an initial period the Member States would apply the basic principles of data protection of the Council of Europe Convention and any problems arising from the fact that protection in Member States was not equivalent would be dealt with by administrative actions such as those foreseen in Articles 27 and 30 in the draft Directive;

- at the end of the initial period and on the basis of the experience gained the Commission would provide a unifying text, possibly even in the form of a Regulation.
9. As regards the *legal basis*, the Irish delegation queried whether it would not be more appropriate that the basis be Article 235 of the EEC Treaty rather than Article 100 A as the Directive was more related to human rights than the internal market. The Irish proposed that the legal service of the Council be asked to pronounce itself on the legal basis.

10. The French delegation in its preliminary remarks indicated that it welcomed the proposal made by the Commission and that it would participate in the work as constructively as possible. The proposal by the Commission did however give rise to a number of difficulties for the French delegation.

   The French delegation had noted not only that the directive allowed Member States which had a higher level of protection than that foreseen by the Directive to maintain such a level of protection, but also that in order to avoid distortion of competition and ensure the free flow of data, it was necessary to have as homogeneous a system as possible. The French delegation agreed with this principle under the condition that the homogeneous approach was made at a high level of protection and took into account national laws which have already been adopted.

   As regards the question of transparency, the French delegation indicated that it attached great importance to assuring a certain amount of transparency in the processing and collecting of personal data and felt that the draft Directive did not go far enough in this respect, especially as regards the guarantees afforded to the data subject: in respect of the creation of files and in respect of the information to be given to the supervisory authorities.
The distinction between the private and public sectors which did not exist in the Council of Europe Convention did not appear pertinent to the French delegation. The French delegation wondered why this distinction had been chosen instead of a distinction based for example on the nature of the files.

Referring to the supervisory authorities the French delegation queried by which legal technical means the obligations flowing from the Directive would be rendered binding on the Institutions of the European Community.

11. The Spanish delegation welcomed the draft Directive proposed by the Commission but expressed concern as to the implications of the Directive in specific sectors as for example tax files and police files. In the Spanish delegation's view specific account would have to be taken of these specific sectors in the Directive.

The Spanish delegation also indicated that although certain fundamental principles were common to the public and private sectors, there did however also exist a number of differences. Whereas, in the public sector standards laid down the conditions under which a file could be used, such standards did not exist in the private sector. They would be created independently and in this respect the Directive had concepts which would be difficult to implement.

The Spanish delegation also mentioned that although the proposal by the Commission used the expression equivalent protection it would allow a certain latitude for the Member States. This could, in the Spanish delegation's view, lead to strange effects.
Finally, the Spanish delegation indicated that it had problems relating to the supervisory authorities foreseen as it did not know exactly what would be the powers of these authorities.

12. The Greek delegation informed the Working Party that although attempts had been made to legislate in the field of personal data protection in Greece since 1979, legislation had not been passed. A draft drawn up in 1986 by a special committee had because of ministerial changes and elections not become law. It was however expected that a draft would very soon be submitted again to Parliament.

As a general comment on the draft proposal by the Commission the Greek delegation underlined the difficulties which might arise when a matter was dealt with by different international organisations. International texts established by the different organisations could be in conflict with each other and give rise to questions of interpretation.

Referring specifically to the intervention by the Irish delegation concerning the legal basis, the Greek delegation queried whether the title of the Directive was appropriate and should not rather refer to the free movement of data.

13. The German delegation welcomed the proposal by the Commission which it considered necessary for the creation of an internal market and which should be based on a high standard going beyond that set out in the Council of Europe Convention. The German delegation particularly welcomed the inclusion of manual data in the scope of the proposed Directive and stressed the need to ensure that it would be possible to maintain specific systems of protection for specific sectors going beyond the
protection foreseen in the Directive. As regards the transfer of personal data to third countries, the German delegation indicated that the provisions proposed by the Commission seemed impractical and that it would make certain alternative proposals in this respect.

14. The Danish delegation thanked the Commission for the initiative it had taken and shared the views of the Commission that it was necessary to create data protection at a high level in order to ensure the flow of data between Member States. The Danish delegation stressed however that it had particular problems with the Directive and that it could not support it as it was presently formulated.

The Danish delegation drew attention to the following points in particular:

- the question whether manual data generally should be covered by the scope of the Directive. Should the Directive include manual data, this would create difficulties in respect of the Danish legislation in the field of data protection;

- the Directive was too bureaucratic by giving detailed procedural rules instead of creating general substantive rules;

- the Directive was unclear in respect of the passing on of information from public sectors to the private sector and within the public sector and in this connection the Danish delegation had noted that the directive did not give specific exceptions for information to be passed on for statistical or scientific purposes. Such exceptions would, according to experience in the Danish delegation's view, be necessary.
The Danish delegation was satisfied that the Directive to a wide extent was based on the principles of the Council of Europe Convention. One could perhaps consider drafting the Directive by referring to the principles of the Convention, following which it would only be necessary to provide supplementary rules concerning the exchange of information between the Member States of the EC and between these States and third countries.

15. The Belgian delegation informed the Working Party that although Belgium had not yet ratified the Council of Europe Convention, Belgium had the intention of ratifying the Convention and a draft law which would transpose into national law the principles of the Convention would be submitted to Parliament shortly. As the other Member States which had not yet ratified the Convention also intended to do so, one could ask if the Directive which in any event could only be a minimal directive, was necessary. As interventions made in the Working Party already showed that whereas some delegations for example were in favour of including manual files, other delegations had expressed opposition to such an inclusion, one could query whether it would be possible to go further than what had already been provided for in the Council of Europe Convention. The Belgian delegation, furthermore, indicated that as certain exceptions in relation to the rules of data protection already existed in the Member States in order to take into account specific problems in those countries, it could be expected that Member States with such exceptions would wish to maintain them.

As it seemed doubtful to the Belgian delegation whether it would be possible to go further than the Convention this delegation wondered if, instead of taking systematically the principles of the Convention and attempting to better them by going further as had been
proposed by the Commission, it would not be more appropriate to take a more pragmatic approach. In this context and referring specifically to Articles 3(2)(a) and 12 of the Council of Europe Convention which allow Member States to make exceptions to the principles of the Convention, the Belgian delegation proposed to examine these exceptions more closely and to see how problems arising from the use of such exceptions could be solved.

As regards the accession of the Communities to the Council of Europe Convention the Belgian delegation expressed the wish to obtain further information as to the contents of any protocol and the legal consequences of any accession by the Communities to the Convention. In this context the Belgian delegation referred to the problems which could arise from the fact that the same subject matter would be dealt with by two different jurisdictions and the fact that the text proposed by the Commission was not compatible with the Convention.

16. As the protection of data was considered as a human rights issue, the Belgian delegation supported the request by the Irish delegation to ask the Legal Service to give an opinion as to the legal basis proposed by the Commission.

17. The United Kingdom delegation stated that it was not yet in a position to express a final view on the Commission’s proposal as consultations of the interested circles were still under way in the United Kingdom.

As a preliminary general remark the UK delegation indicated that when considering the question of data protection it had to be borne in mind that a modern society was built on information and the circulation of information. Taking this as a starting point, information
should be free and it was consequently necessary to strike a balance between the need to protect privacy and to ensure the free circulation of information.

The question of general restrictions on the free flow of information had only become acute with the introduction of computers and this had to be borne in mind when looking at the future scope of legislation in the field of data protection. As data protection laws in any form impose burdens both on government administration and on commerce, one should strive for sensible measured objectives, for solutions proportionate to the scale of problems caused, and for procedures which were simple for the users of data and data subjects.

The United Kingdom marked a preference that the directive should address the problems posed by particularly computerized data rather than the whole field of privacy.

18. Whereas certain proposals made by the Commission seemed sensible to the UK delegation, others worried the UK delegation. The worrying issues in particular concerned:

- the concepts of the Directive which were very general and which would have to be qualified by very general exceptions would be difficult to translate into practice;

- the notification system for some data;

- the concept of self-determination;

- the restrictions on disclosure to third parties which were likely to be burdensome and which might prove to be counter-productive in the case of some industries;
- the extension to manual data which seemed unjustified;

- the codes of conduct which could become too inflexible;

- the exceptions - should the holding of data for domestic purposes, payrolls, accounts, be subject to the rules of the Directive?

The UK delegation finally indicated that it was still examining the question of the legal basis of the proposed Directive.

19. The Netherlands delegation stated that the document submitted by the Commission was an extremely important one. It would however have wished that the proposal had been discussed in other fora before being submitted to Council. In general terms the Netherlands delegation was in favour of the proposal by the Commission. The Netherlands delegation:

- felt, however, that certain provisions were too cumbersome and left open the question of how much discretion was left for Member States;

- felt that the proposals raised the question of what equivalent protection in the context of a Directive really meant;

- felt that the Directive raised the question of the appropriateness of establishing rules concerning the approval of the person concerned before information was used;

- asked what was meant by providing that the Directive would apply to the public sector with the exception of files in the public sector where activities of this
sector did not fall within the scope of Community law and this especially when seen in relation to the Schengen Agreement.

The Netherlands delegation expressed the wish that the draft Directive be examined article by article and principle by principle scrutinizing what the problems involved really amounted to in practical terms.

20. The Luxembourg delegation informed the Working Party that Luxembourg, since 1979, had a law on personal data protection. Luxembourg was, however, reflecting on the possibility of readjusting its legislation because of the progress made in the field of automatic data processing. This adjustment would however await the progress made in the Working Party. The Luxembourg delegation went on to explain that the Luxembourg law at present did not include manual files but questioned whether it would not be more appropriate to include such files. Whereas the Luxembourg law made a distinction between the public and private sectors proposed by the Commission in its draft directive, this distinction did not apply to the protection itself but to the protection procedures.

In the Luxembourg delegation's view protection of personal data should be considered as a whole and this in respect of - the time of protection which should start already from the collection of data - the nature of data, i.e. manual or automatic files - data in the private and public sectors. If there was equivalent protection in all Member States this equivalence should be attached to the main principles of data protection concerning:
- the end results sought by the processing of data;
- the transparency of this processing;
- and an independent control.

Although it could be said that all these principles for the protection of data were already contained in the Council of Europe Convention, it could equally be argued that the Convention only established a philosophical framework and that within the European Communities such a framework would not suffice and more specific and more precise rules would be necessary.

IV. Reactions of the Representative of the Commission to the general remarks by delegations

21. Reacting to the general remarks made by delegations, the Representative of the Commission noted with satisfaction that there was general support for the fact that the Commission had made a proposal for data protection and that a large number of elements of the Commission's proposal had been supported. Responding specifically to certain questions and doubts which had been expressed the Representative of the Commission explained:

- that as regards the inclusion of manual files it had been advanced that the question of data protection had only become acute with computerization. Although this might be true it did not however mean that problems did not exist also in the area of manual files and this especially in respect of the access and transmission of data. When the Commission used the term manual files it meant files which had characteristics coming very close to automatic files;
that the Directive aimed at obtaining equivalent protection. Such an equivalent protection was necessary in order to permit the free flow of data between Member States. It would however be possible for Member States to provide a higher level of protection than that foreseen in the Directive. A protection going too far could however entail competitive disadvantages for those States going beyond the level foreseen in the Directive. The possibility of providing a higher level of protection could however not impede the guarantees of free flow of data between the Member States;

that the distinction between the public and private sector was based not so much on a distinction between sectors but more on a distinction between public functions and private functions. The basis for public functions were to a great extent different from those of private functions;

as to the Directive being too bureaucratic, this to a large extent depended on how it was implemented in practice;

that the accession of the Communities to the Council of Europe Convention required Community legislation to be established ensuring protection at the same level or beyond that required by the Convention. As the Convention at present only made accession by States possible a protocol would have to be negotiated allowing the accession of the European Communities;

as to the incompatibility between the Directive and the Convention there was none;
- that as far as the legal basis was concerned, Article 100 A of the EEC Treaty provided the appropriate basis in as much as a high level of equivalent protection was essential to the creation of the internal market. Consequently recourse to Article 235 of the EEC Treaty would not be possible as this was a subsidiary provision used only when no legal basis had been foreseen in the Treaty. As to the possibility of requesting the legal services of the Council or the Commission to give an opinion on the legal basis it would be premature as the final contents of the Directive were not yet known.

V. Discussion of Article 1

a. Structure

22. Discussing the structure of Article 1, the Working Party took note of a suggestion by the French delegation to invert the order of paragraphs 1 and 2. In the French delegation’s view it would be more logical to start with the real general principle of the Directive to ensure the free flow of personal data between the Member States and then to speak in paragraph 2 of the protection of privacy of individuals which could constitute an obstacle to the free flow of data.

Responding to the suggestion made by the French delegation the Representative of the Commission explained that the principle of the Directive was that only once an equivalent protection of personal data in the Member States had been achieved could one require the free flow of such data between the Member States. As equivalent data protection formed a condition for free flow it was consequently logical that the principle of free flow be given after the principle of equivalent data protection as suggested by the Commission.
For the Greek delegation the philosophy of the Commission could be clarified by adding in paragraph 2 the words, "given that Member States have established data protection".

The Chairman of the Working Party suggested inserting in paragraph 1 the words "equivalent protection" thus setting the principle that with equivalent protection in all Member States the necessary guarantees existed for not preventing the free flow of personal data.

b. Wording of Article 1, paragraph 1

23. As regards specifically the discussion of paragraph 1 of Article 1, the Working Party noted:

(a) that a number of delegations felt that the notion "privacy of individuals" proposed by the Commission was too restrictive. It was suggested either to use the term "interests of individuals" or "individual rights";

(b) that certain delegations felt that the word "processing" was too narrow as also the collection of data ought to be covered;

(c) that the Belgian delegation proposed, at least in the French text, to speak of "personnes physiques" instead of just "personnes";

(d) that in the Luxembourg delegation's view the term "data files" seemed outdated.

As regards the use of the words "privacy of individuals" the Representative of the Commission indicated that these words corresponded to the wording of Article 8 of the Human Rights Convention. If this wording was not
completely satisfactory the Representative of the Commission would be prepared to accept the wording "in particular the privacy of individuals". As regards the remarks set out under (b), (c) and (d), the Commission suggested that these points be better discussed when dealing with Article 2 of the draft Directive.

c. Scope of paragraph 2

24. Discussing Article 1, paragraph 2 and especially the scope of this provision, the Representative of the Commission reiterated that the proposal of the Commission followed the principles laid down by the Court of Justice in the "Cassis de Dijon" ruling. The Directive would set out an adequate level of protection without however preventing Member States from going even further. This would avoid harmonizing all aspects in all details. Such an approach did not however allow obstacles to be made to the free flow of data from or to a State which had opted for a higher level of protection than that required by the Directive.

Whereas certain delegations indicated that they could accept the principle outlined by the Representative of the Commission, a number of other delegations felt that such an approach would render the national laws of the Member States which had introduced a higher level of protection than that required by the Directive a dead letter. Reference was in this context also made to the fact that the Council of Europe Convention in its Article 12 allowed exceptions to the general principle of free flow of data information.
VI. Future work

25. At the next meeting of the Working Party discussions will be devoted to Chapters I and V of the Commission's proposal for the protection of individuals in relation to the processing of personal data.

Scheduled meetings of the Working Party (Economic Questions) protection of personal data

Meetings scheduled for the discussion of the Directive on the protection of individuals in relation to processing of personal data:

27 and 28 (morning only) March 1991
2 and 3 May 1991
19 and 20 June 1991.

Meetings scheduled for the discussion of the proposed Directive concerning the protection of personal data in the context of public digital telecommunications interests, in particular the integrated services digital network (ISDN):

22 April 1991
3 and 4 June 1991.
OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Data Protection)
on: 22 April 1991

No. prev. doc.: 5705/91 ECO 49
No. Cion prop.: 8460/90 ECO 158 COM(90) 314 final - SYN 287-288

Subject: Protection of individuals in relation to the processing of personal data


I. Introductory remarks

2. Having taken note of the introductory remarks by the representative of the Commission explaining the reasons for and the contents of the proposed Directive, the Chairman of the Working Party recalled that for the purpose of a useful discussion it should be borne in mind that whereas directives were binding as to the results to be achieved in each Member State, the choice of form and methods were left to the national authorities. He consequently proposed as a first stage to discuss the question of substance in order to reach agreement on the aims and results of the Directive and then, at a second stage, examine the different articles in order to come to an
agreement on the form and wording of the Directive. The Chairman furthermore proposed to structure the Directive in the way set out in the Annex to the present document.

II. General reactions from delegations to the proposed Directive

3. The United Kingdom delegation, although understanding the reasons and the logic for the Commission to table the proposed Directive, felt that the Directive as presently worded went into far too much detail and might prove to be unworkable. Furthermore, the Directive did not, in the UK delegation's view, strike the right balance between the needs of the telecommunications organisations and the privacy rights of individuals. Referring specifically to Articles 4, 5, 9 and 10, the UK delegation indicated that the purposes referred to in these articles were too restrictive and suggested that they be made simpler and more permissive. Also Articles 12 and 13 seemed too complicated and needed to be stripped down to essentials. As far as Article 11 was concerned this Article was unacceptable to the UK delegation.

For the UK delegation the proposed Directive also gave rise to two problems of a more structural nature — one concerning the way in which it was linked with the General Directive and the second concerning the fact that the proposed Directive seemed to place the responsibility of how the obligations of the Directive were to be met on the telecommunications organisations and not on the Member States.

The UK delegation finally suggested a general debate on whether the proposed Directive should focus narrowly on telecommunications organisations.

4. The Belgian delegation indicated that it was still examining the proposed Directive in order to fix its position. It wondered, however, if it was not premature to examine the "Telecommunication networks Directive" as the discussion of the General Directive was still at a very preliminary stage. In
this context the Belgian delegation furthermore recalled that it had asked for a legal opinion as to the legal basis of the General Directive and indicated that it also had certain misgivings as to the legal basis for the proposed telecommunications networks Directive under discussion.

5. The Netherlands delegation, although acknowledging the importance of harmonizing rules to ensure the protection of privacy in the Community and ensure an open market for services, wondered if the proposed instrument would accomplish these aims. Taking into account that the main Directive was not yet approved and that the telecommunications networks Directive at present with its very detailed and inflexible rules risked being overtaken by the technological evolution, the Netherlands delegation suggested that a better approach would be that of "self regulation" within specific areas setting certain basic principles and leaving a certain degree of responsibility to the specific area chosen.

Referring specifically to the text of the Directive, the Netherlands delegation drew attention to the problems that the interaction between the main directive and the telecommunications Directive could give rise to and the problems arising from the different wording used in the two Directives.

The Netherlands delegation furthermore stressed

- the need to deal with data protection in a wider context and not just link it to the area of telecommunications organisation;

- the cost element of covering also services based on analogue networks;

- the need to decide whether legal and natural persons should be subject to the same rules of protection.
The Netherlands delegation finally queried whether the EC had powers in the area of ensuring the protection of privacy.

6. The French delegation welcomed the proposal by the Commission which met not only a real need to harmonize rules within the EC but also the ever increasing feeling among consumers for the need to obtain protection of personal data and privacy in light of technical evolution. The French delegation in this context stressed the importance of also including the protection of privacy within the scope of the Directive. For the French delegation the proposed Directive was however not coherent and should, in the French delegation's view, not only cover public telecommunication services but should be enlarged to apply to all suppliers of services. Acknowledging that a certain amount of detail was necessary the French delegation felt however that the Directive went beyond "the essential requirements" by imposing too many restrictions with a consequential cost increase.

7. The Irish delegation indicated as a preliminary view that the principles set out in the proposed Directive were laudable but that the provisions as presently formulated would give rise not only to a number of commercial but also technical and financial problems.

8. The Italian delegation indicated that it had not yet a final view on the proposed Directive but agreed with the view expressed that the scope of the Directive should not be limited to the public sector but extended to include all providers of services. The Italian delegation stressed the need in the Directive to make a clearer distinction between the rules on the use of data and the rules concerning the contents and drew attention to the important question of the costs related to the implementation of the Directive in respect of services based on analogue networks. Bearing in mind that a very low percentage of the Italian network at present was digital, the Italian delegation also raised the question of the time given to Member States to comply with the Directive.
9. The Danish delegation thanked the Commission for the initiative it had taken indicating that it shared the views of the Commission on the need for Community rules in the area proposed by the Commission. Although the main objective of the Directive could be supported, the Directive did however contain a number of requirements which would be difficult to fulfill and highly costly to implement. The Directive should in the Danish delegation's view attempt to strive to combine considerations related to the protection of privacy with considerations related to what was technically and administratively feasible. More specifically the Danish delegation indicated that it seemed inappropriate to put the responsibility on the telecommunications organisations for matters which were not of their concern. The Danish delegation finally indicated that it did not find the "committee arrangement" foreseen in the proposed Directive as adequate.

10. The Greek delegation welcomed the proposal by the Commission but indicated that it was not yet in a position to take any final stand on it as the examination of it had not yet been completed.

11. The German delegation also welcomed the initiative taken by the Commission which, in the German delegation's view, went in the right direction. It would however be necessary, when examining the different provisions, to see if the right balance had been struck between the interests of the consumers and those of the operators. The German delegation also agreed with the view expressed by a number of delegations that the scope of the proposed Directive should not be limited to the public sector but be extended to all providers of services.

12. The Spanish delegation indicated that it agreed with the Commission on the urgency of arriving at a result within the area covered by the Directive but regretted that studies on the implementation at national/international level in the area covered by the proposed Directive were not available. In the absence of such studies and taking into account the link to the
General Directive, the Spanish delegation suggested that the best means of making headway in discussions would be for the Working Party to concentrate on the technical aspects of the Directive and especially Chapters III and IV (in the structure proposed by the Chairman set out in the Annex).

III. Discussion of Chapters I and III

Chapter I

13. Title

Referring to the title of the Directive as proposed by the Commission, the French and Spanish delegations indicated that the title might lead to confusion as it referred to public digital telecommunications networks whereas Article 2 stipulated that the provisions of the Directive would also apply to services based on analogue networks. The French delegation consequently proposed to use a more general term referring just to "telecommunications services".

Article 1: Object of the Directive

14. Discussing Article 1 the Working Party noted

- a suggestion by the Spanish delegation to use in paragraph 1, as had been done in paragraph 2, the term "protection of personal data and privacy";

- agreement to reflect on the possibility of replacing in certain linguistic versions the words "equal level of protection" by the words "equivalent level of protection" as used in the French text;

- a proposal by the UK delegation to clarify that the main objective of the Directive was that of free movement of telecommunications equipment and services between Member States;
that the Irish delegation on the other hand suggested replacing the words "provide for the free movement" by "contribute to the free movement" as the main purpose of the Directive, in this delegation's view, was not that of providing for the free movement but that of protecting privacy;

- that a number of delegations felt that the inclusion of the reference to protection of privacy was necessary in order to cover, for example, malicious calls and call forwarding;

- a proposal by the Danish delegation to qualify the scope of the Directive more precisely already in Article 1.

Articles 2 and 3

Article 2 paragraph 1

15. Referring specifically to the opening sentence of Article 2 paragraph 1 ("Without prejudice to the general provisions of Council Directive") the UK delegation stressed the need, once discussions had come closer to the final stages, to review the Directive on telecommunications networks in order to ensure that there were no contradictions with the main Directive.

16. In connection with the discussion of paragraph 1, certain delegations also indicated that the scope of the Directive, by referring to the provision of public telecommunications services in digital telecommunications networks, was too restrictive.

Article 2 paragraph 2

17. Discussing Article 2 paragraph 2 and referring specifically to the inclusion of services based on analogue networks, a number of delegations reiterated their concern, as expressed in their general comments, with the financial
implications of such an inclusion. It was in this context proposed, when examining the different provisions of the Directive, to see if and how these provisions could also be applied to analogue networks.

18. The Spanish delegation furthermore suggested rewording paragraph 2 of Article 2, which gave the impression that once a Member State had implemented the Integrated Services Digital Network there would no longer be problems related to analogue networks, whereas the fact was that analogue networks would still remain for a number of years even after a State had begun the introduction of ISDN.

19. Discussing Article 2 a number of delegations also reiterated their view as expressed in their general comments of not limiting the scope of the Directive to public telecommunications services. Reference was in this context also made to the definition in Article 3(2) which in certain delegations' views should also include private bodies who did not provide telecommunications services on the basis of an exclusive right. In this connection a request was made for aligning Article 3(2) and (4).

As a consequence of the remarks made related to the too narrow scope of application proposed by the Commission, the French delegation proposed to provide in Article 2 for a larger scope and then in the different provisions of the proposed Directive to examine their applicability to telecommunications organisations and other providers of services who did not possess any exclusive rights. In this context the Luxembourg delegation proposed that Article 2 be reworded by referring only to users of networks and providers of services.

20. Responding to the remarks made relating to Article 2, the representative of the Commission indicated that the Commission had chosen a pragmatic and flexible approach concentrating the scope of this Directive on the main problems i.e. those related to the telecommunications networks. As to the request that the
21. As to the problems related to cost aspects of the implementation of the Directive in relation to services based on analogue networks, the representative of the Commission acknowledged the existence of these problems and did not exclude the possibility of providing for either derogations or transitional periods.

Article 3

22. As regards specifically Article 3, the Italian delegation proposed to introduce a definition of "privacy".

The Chairman of the Working Party, in order to overcome the problem of whether the Directive covered natural as well as legal persons, proposed to speak of "subscriber".

Chapter III

Article 12

23. From the discussion of Article 12 it emerged that for a number of delegations this provision gave rise not only to questions concerning the legal/philosophical approaches underlying this provision and in particular the over-emphasis of the protection of the caller - but also raised problems as to its practical implications and the cost involved thereby. It was in this context advanced that Article 12 was an excellent illustration of the need which had been expressed when...
discussing the scope of the Directive to examine case by case to which extent the different provisions of the Directive should apply, for example, whether analogue networks should be included or not.

24. Discussing Article 12 the question of the link between this provision and type requirements was also raised.

25. Responding to the comments made by delegations, the representative of the Commission explained that it had sought to protect equally the caller and the called. It was because of this need to strike the right balance that a number of situations and hypotheses had to be covered and it was consequently not possible to simplify the provision as had been suggested.

26. As to the relation to type requirements, the representative of the Commission explained that a distinction would have to be made between subparagraphs 1 and 2 of paragraph 2 in Article 12. Whereas one could envisage that the terminal equipment should be able to fulfil certain conditions established by the Directive, one could envisage that other requirements (second subparagraph) be fulfilled by the networks in order not to oblige subscribers to buy expensive equipment.

27. As to the general costs aspect of the implementation of the rules foreseen in Article 12, the representative of the Commission reiterated that it could be examined whether transitional periods for implementation would be necessary.

Article 13

28. From the discussion of Article 13 on which a number of delegations reserved their position and on which only preliminary views were expressed, it emerged that certain delegations felt that as the provision was related to penal law which fell within the competence of Member States, a clear reference to national legislation would be necessary.
Redrafting would also be necessary to avoid the impression which the present wording gave that the obligations provided for were to be carried out by the telecommunications organisations and were not subject to a request by a public authority.

29. Reacting specifically to a question by the Irish delegation as to the use of the words "for a limited period of time" in Article 13 paragraph 1 first sentence, the representative of the Commission explained that they were not to be interpreted as meaning a short period but implied that the subscriber was contacted periodically in order to establish if there was still a reason for overriding the elimination of the calling line identification.

30. Discussing Article 13 paragraph 2 the UK delegation proposed to include also persons who were subject to bomb or terrorist threats under the permanent override function. In relation to the discussion of Article 13 paragraph 2 the question of the practical possibilities of implementing paragraph 2(b) was also raised.

31. Responding to the reactions by delegations the representative of the Commission indicated that as far as the link with national penal law was concerned, the intention of the provision was that it should be for the national courts or authorities, by applying national rules, to decide whether measures such as those foreseen in Article 13 were to be taken. He furthermore suggested redrafting Article 13 by indicating that the States should take all necessary measures to ensure that telecommunications organisations were able to comply with the requirement of Article 13.

32. Discussing Article 14 a number of delegations wondered if the rules provided for in this Article could be considered as an essential requirement and whether it was at all necessary
that a rule on forwarding of calls as proposed and which in any event would create difficulties as to its implementation be included in the Directive.

33. Referring specifically to a criticism made in relation to Article 14 paragraph 2 that the procedure foreseen could constitute an encouragement to burglary, the representative of the Commission stated that the Commission attached great importance to this provision which was necessary to maintain a symmetry on the protection of the caller and the called.

Article 15

34. As regards Article 15 certain delegations, as had been done when discussing Article 14, queried the need for such a provision which did not seem possible to implement. These delegations requested the suppression of this provision.
Chapter I

General provisions

Article 1 Object of the Directive
Article 2 Scope
Article 3 Definitions

Chapter II

Lawfulness of processing in the telecommunication sector

Article 4 Principles
Article 5 Aims
Article 6 Right of access
Article 7 Confidentiality
Article 8 Security
Article 9 Billing
Article 10 Traffic data
Article 11 (to be integrated into Article 9)

Chapter III

Technical provisions to ensure the protection of privacy of the users

Article 12 Right of identification of the calling and called subscriber
Article 13 Derogations to the right of identification of the calling and called subscriber
Article 14 Obligations to inform when calls are forwarded
Article 15 Obligations to inform when third parties have access

Chapter IV

Telecommunication services

Article 16 Teleshopping
Article 17 Canvassing
Article 19 Other services
Article 20 Other service providers

+ The UK delegation proposed a sub-division of Articles 4, 5, 9 and 10.
Chapter V

Provisions concerning the implementing of the Directive

Article 18  Technical features and standards
Article 21  Administrative and technical modalities

Chapter VI

Working Party on Protection and Advisory Committee

Article 22  Working Party on Protection
Article 23  Advisory Committee

Chapter VII

Final Provisions

Article 24  Bringing into force of the Directive
Article 25  Addressees of the Directive
EUROPEAN COMMUNITIES
THE COUNCIL

Brussels, 17 December 1991 (OR.nl)
10203/91

RESTREINT
ECO 197

COMMUNICATION

from : Presidency

to : Internal Market Council

Subject: Protection of individuals in relation to the processing of personal data and information security

I. General

On 27 July 1990, the Commission submitted to the Council six documents on the above subject, including:

- a proposal for a Council Directive on the protection of individuals in relation to the processing of personal data (SYN 287);

- a proposal for a Council Directive concerning the protection of personal data and privacy in the one text of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks (SYN 288);

- a proposal for a Council Decision in the field of information security.

The first proposal for a Directive (the "framework Directive") is designed to harmonize the laws, regulations and administrative provisions of the Member States on the protection of individuals in relation to the processing of personal data, in order to ensure free movement of personal data within the Community. The three documents not listed above are related to that proposal.
The second proposal for a Directive is designed to flesh out and supplement the framework Directive in the field of telecommunications using digital networks.

The last proposal provides for a Community action plan in the field of information security.

On 17 September 1990, the Internal Market Council held an initial discussion on these proposals.

The proposals are still under discussion at the European Parliament. The Economic and Social Committee delivered its Opinion on 24 April 1991.

II. Discussions in the Working Party on Economic Questions

The Working Party on Economic Questions (Data Protection) gave priority under the Netherlands Presidency to continuing with discussions on the framework Directive and the proposal on information security.

At the meetings on 23 and 24 July, 19 September and 7 and 8 October 1991, the Working Party completed the first reading of the proposal for a framework Directive. Particular attention was paid to Chapter VIII on the transfer of personal data to third countries.

After completing the first reading of the framework Directive, the Working Party gave precedence to discussion of some key issues in the Directive, particularly as regards the structure and content of Chapters II and III on the lawfulness of processing in the public and private sectors.

Such discussion took place at the meetings on 12 and 13 November and on 12 and 13 December 1991, on the basis of a working document from the Working Party's Chairman.

A central issue here was how to strike the right balance between the envisaged Community measures and national legislation in this field. Discussions also addressed the relationship between substantive principles and the various methods of ensuring their application.

At the Working Party's request, the Legal Service gave an opinion in writing on the legal bases for the proposal for a framework Directive. This point will need to be discussed in more detail by the Working Party.
At the meeting on 20 September 1991, discussion of the proposal on information security was virtually completed. Further progress here depends on the European Parliament's Opinion.

The incoming Portuguese Presidency stated at the meeting on 12 and 13 December 1991 that it attached equal importance to this dossier and that it would endeavour to see that the Working Party continued to meet with the same frequency. The Working Party noted this and recorded its agreement.

III. Proposed conclusion

Pending the continuation of the Working Party's proceedings, it will suffice to take note of this communication.
EUROPEAN UNION
THE COUNCIL

Brussels, 23 June 1994 (27.06)

7966/94

RESTREINT

ECO 156

TRANSLATION OF LETTER

from : Commission of the European Communities, signed by Mr René STEICHEN, Member
dated : 14 June 1994
to : President of the Council of the European Union

No. Cion prop.: 8460/90 ECO 158 COM(90) 314 final SYN 287-288

Subject: Amended proposal for a European Parliament and Council Directive concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and digital mobile networks

Sir,

I would inform you that, in response to the Opinions of the European Parliament and the Economic and Social Committee, the Commission has decided, under Article 189a(2) of the Treaty establishing the European Community, as amended by the Treaty on European Union, to amend the proposal for a European Parliament and Council Directive concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and digital mobile networks, which it submitted to the Council on 27 July 1990 (COM(90) 314 final SYN 288, as amended by COM(92) 422 final SYN 287).
The purpose of the amended proposal is to simplify the original proposal and comply with the principle of subsidiarity.

The text of the amendments is enclosed.

(Complimentary close).

For the Commission

(s.) René STEICHEN
Member

Encl.: COM(94) 128 final COD 288
OUTCOME OF PROCEEDINGS

from: Working Party on Economic Questions (Telecommunications)
dated: 27 January 1995

No. prev. doc.: 7966/94 ECO 156 : COM(94) 128 final - COD 288
Subject: Amended proposal for a European Parliament and Council Directive concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and digital mobile networks

I. INTRODUCTION

Following presentation of the amended proposal by the Commission, the Working Group on Economic Questions (Telecommunications) held a preliminary exchange of views on the matter at its meeting on 27 January 1995.

The Commission representative stressed the importance of identifying the differences between the draft general Directive on data protection and the proposed specific Directive.

- The general Directive provides a broad framework and covers all sectors where processing of personal data could take place, including telecommunications. It is limited to setting the broad principles and leaves the greatest possible freedom to the Member States for implementation.
- The specific Directive aims to apply the general principles of the protection of personal data and privacy with regard to the specific requirements of digital telecommunications networks in order to prevent divergent developments in the Community which could endanger the common market for both telecommunications services and terminal equipment.

The relationship between the general Directive and the specific Directive on data protection should be summarized by three principles:

- specificity: the Directive relating to digital telecommunications networks is limited to this sector;
- consistency: for the sake of consistency, the specific Directive uses the same concepts and the same definitions as the general Directive;
- complementarity: measures are complementary, without repeating the provisions contained in the general Directive.

II. INITIAL REACTIONS OF THE DELEGATIONS

Most delegations made general comments on the amended proposal, mainly in relation to whether there was a need for a specific instrument in this field at this stage. Some delegations were in favour of such an instrument (B, GR, I, L, A), whilst others were sceptical (DK, NL, FIN) or opposed (UK). Concerning the contents of the provision, one delegation (P) was critical of the proposed provisions.

However, the majority of delegations were of the view that it was not appropriate to start examining in detail the text of this specific Directive before having a more definitive text of the general Directive on data protection (after formal adoption of the Common position by the Council and second reading by the European Parliament).
III. CONCLUSION

Whilst awaiting progress on the general data protection Directive, the Presidency invited delegations to reflect on the general principles of the amended proposal and also to examine the specific measures, bearing in mind the whole context of the Information Society and the rapid technological evolution within the telecommunications sector.
RESULTATS DES TRAVAUX

du : Groupe "Télécommunications"

en date du : 12 juillet 1995

n° doc. préc. : 4739/95 ECO 21
n° prop. Cion : 7966/94 ECO 156 COM(94) 128 final COD 288

Objet : Proposition modifiée de directive du Parlement européen et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux numériques de télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques

Lors de sa réunion du 12 juillet 1995 le groupe a repris l'examen\(^{(1)}\) de la directive mentionnée en objet qu'il avait différé en attendant que les travaux sur la directive générale soient finalisés. \(^{(2)}\)

1. Remarques générales

Ces remarques restent préliminaires, la plupart des délégations ayant fait savoir qu'elles n'avaient pas encore achevé leurs consultations internes sur la directive.

---

\(^{(1)}\) Le groupe a entamé l'examen de cette directive le 27 janvier 1995, cf. doc. 4739/95.

\(^{(2)}\) La directive générale a été définitivement arrêtée par le Conseil le 24 juillet 1995.
Les délégations A, B, I et L ont fait savoir que, globalement, elles étaient en faveur de la proposition modifiée même si elles regrettaient qu'elle fait une part trop importante à la subsidiarité (A et L ont notamment souhaité la réintroduction de l'article 4 de la proposition initiale).

La délégation F s'est également exprimée en faveur de cette proposition mais elle considère que beaucoup d'amendements sont nécessaires pour tenir compte de l'environnement concurrentiel post 1998. Elle estime par ailleurs qu'une analyse coûts/bénéfices s'impose pour bon nombre des mesures prévues, en particulier dans le cas où des options sont offertes gratuitement aux usagers.

Les délégations DK, NL et UK de leur côté se sont interrogées sur la nécessité de bon nombre des dispositions envisagées, DK et UK exprimant même des doutes sur le principe d'une directive spécifique au secteur des télécommunications alors qu'un code de conduite pourrait selon elles suffire.

2. Observations portant sur les articles

Le groupe a examiné les onze premiers articles.(3)

Article 1er : Objectif

Un consensus s'est dégagé en faveur d'un alignement du texte de cet article sur celui de la directive générale.

Par ailleurs UK, qui déclare avoir des difficultés pour concevoir la notion de données personnelles d'une personne morale, s'est opposée à l'extension de la directive aux personnes morales.

(3) A noter que la base juridique proposée (article 100A) n'a pas soulevé d'objections, UK ayant toutefois estimé que selon elle certaines dispositions proposées ne pouvaient pas être basées sur cet article.
La Commission, notamment appuyée par B, a insisté pour le maintien des personnes morales et s'est offerte à proposer une définition des personnes morales.

**Article 2 : Définition**

Afin de mettre les définitions en cohérence avec l'environnement concurrentiel post 1998, le président a présenté les modifications suivantes :

- supprimer les définitions des termes "organisation des télécommunications" et "prestataire de services" ;

- modifier comme suit la définition de "réseau de télécommunications public" : "système de transmission et, le cas échéant, équipement de commutation et autres ressources permettant le transport de signaux entre des points de terminaison du réseau définis, par fils, par radio, par des moyens optiques ou d'autres moyens électromagnétiques, qui sont utilisés entre autres pour fournir des services de télécommunications publics" ;

- modifier comme suit la définition de "service de télécommunications public" : "un service dont la prestation consiste pour tout ou partie à transmettre et à acheminer des signaux sur des réseaux de télécommunications, à l'exception de la radiodiffusion et de la télédiffusion qui sont accessibles au public".

Ces propositions ont reçu un accueil positif de la part des délégations.

Toutefois F, bien qu'appréciant ces propositions, s'est interrogé sur l'opportunité d'établir les définitions qui doivent servir de base au nouvel environnement réglementaire des télécommunications, dans le cadre d'une directive portant sur la protection des données ; UK a estimé que les modifications vont dans le sens mais a fait savoir que ces nouvelles définitions ne répondaient pas à toutes les questions qu'elle se pose au sujet de l'application de la directive aux prestataires de services.
I a rappelé de son côté qu'il existait une recommandation du Conseil de l'Europe en matière de télécommunications, qui, à ses yeux, constituait une base de référence très utile pour les présents travaux.

**Article 3 : Services concernés**

**Paragraphes 1 et 2**

Le président a proposé de fusionner ces deux paragraphes de la manière suivante :

"Sans préjudice des dispositions de la directive ... [relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données], la présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications publics dans les réseaux de télécommunications numériques publics dans l'Union européenne, en particulier via le réseau numérique à intégration de services (RNIS) et les réseaux mobiles numériques publics."

B s'est déclarée réticente sur la limitation aux réseaux publics numériques de télécommunications, F se demandant de son côté s'il ne serait pas utile de mieux préciser ce que l'en entend par "numériques".

I et UK ont exprimé des objections à l'égard les mots "sans préjudice", figurant au début de ce texte, tout en adoptant un même point de vue différent sur le rapport qui doit exister entre la directive générale et la présente directive.

D'autres délégations étant intervenues sur ce problème de la relation entre les deux directives, il est apparu souhaitable que cette question soit clarifiée pour la suite des travaux sur cette proposition.

La Commission s'est déclaré prête à présenter un texte s'inspirant du considérant n° 9 de sa proposition.
Paragraphe 3

Afin de rencontrer les objections ou les perplexités exprimées par plusieurs délégations, le président a proposé de compléter l'expression "lorsque cela est techniquement possible" par les mots "et économiquement viable", cette suggestion ayant fait l'objet d'un préjugé favorable de NL et P.

Article 4 : Sécurité (4)

Cet article dans sa formulation actuelle suscite les interrogations de la plupart des délégations.

La Commission a proposé de clarifier cette disposition soit en se référant à l'article 17 de la Directive générale soit en reprenant le contenu de cet article ; les délégations B, D, DK, GR, I et S se sont montrées ouvertes à l'égard de cette solution ; UK de son côté a insisté pour la suppression de cet article.

Article 5 : Données de facturation

Paragraphe 1

B appuyée par A et NL a suggéré l'expression "seules les données", que toutefois la Commission a considéré comme non appropriée.

D considère que la durée de stockage de ces données devrait être fixée par référence "aux fins de télécommunications" ; A, B et NL l'ont appuyée.

I de son côté a demandé de mieux aligner le texte de ce paragraphe sur les dispositions correspondantes de la directive générale.

(4) Le président a suggéré de remplacer dans cet article (ainsi que dans les articles 6, 8 et 9) l'expression "organismes de télécommunications" par "prestataires de service public de télécommunications" (provider of the public telecommunications services).
UK a exprimé des réserves sur la dernière phrase qu'elle considère trop limitative. (Il a fait observer que l'article 16 de la directive cadre doit permettre de supprimer cette phrase, B de son côté a insisté pour son maintien).

**Paragraphe 2**

B, appuyée par A et NL, a suggéré d'ajouter après "n'est autorisé" les mots "s'il est nécessaire et au plus tard".

P a exprimé une réserve sur ce paragraphe et proposé de se référer à la date à laquelle une contestation a été définitivement tranchée par les autorités compétentes.

La Commission s'est déclarée ouverte à toute formulation alternative dans la mesure où l'on maintiendrait le principe d'une durée limitée pour le stockage des données de facturation.

**Article 6 : Données relatives au trafic**

Plusieurs délégations (notamment I et UK) se sont interrogées sur la portée précise de cet article.

**Article 7 : Facturation détaillée**

B, D, I, L et NL ont estimé que l'article correspondant de la proposition initiale protégeait mieux la vie privée (par la suppression d'un nombre suffisant de chiffres pour rendre impossible l'identification). I a proposé de dire que la facture détaillée est seulement établie à la demande de l'abonné.

DK, IRL, P et UK ont souhaité que la question reste du ressort des Etats membres.
Article 8 : Identification de la ligne appelante

La Commission a confirmé, à la demande de P, que cet article n'impose pas l'obligation de prévoir un service d'identification de la ligne appelante. Par ailleurs elle s'est montrée ouverte à la suggestion de P de restructurer cet article de façon à ce qu'il soit clair que les différents paragraphes concernent le cas d'une offre d'identification de la ligne appelante.

Paragraphes 1 et 2

UK a soulevé la question de l'applicabilité de ces dispositions dans le cas d'appels concernant les pays tiers.

Il s'est interrogé sur le caractère approprié de la référence faite à la transmission de numéros, et a suggéré par ailleurs de fusionner ce paragraphe 1 avec le paragraphe 2, en ajoutant à la fin du premier paragraphe les mots "ou ligne par ligne" et en supprimant le paragraphe 2.

Paragraphe 3

F, P et UK, dont les préoccupations sont également partagées par B, ont déclaré qu'elles ne pouvaient pas accepter la gratuité de l'élimination ligne par ligne de l'identification, F ayant fait remarquer que cela peut être réglé au niveau des terminaux.

NL de son côté a estimé que le principe de la gratuité ne doit pas permettre les abus dans ce domaine (cas d'abonnés demandant fréquemment des modifications).

Paragraphe 5

P a maintenu une réserve d'examen sur cette disposition.
Article 9 : Dérogations

Paragraphe 1

La Commission a proposé de remplacer, au point a) 5ème ligne, les mots "seront mises à la disposition" par "restent à la disposition", et de supprimer, au point b) l'adjectif "graves", cette dernière demande ayant été appuyée par E.

B s'est opposé à la suppression de "graves" et a suggéré par ailleurs de remplacer "tribunal" par "juridiction" ou par "tribunal ou cour".

UK a accepté le texte de ce paragraphe tout en se montrant réticente à ce qu'on parle au 1b) de "demande expresse".

Paragraphe 2

UK a proposé de fusionner les points a) et b).

Par ailleurs il a été suggéré de parler au début de ce paragraphe de "simple demande".

Paragraphe 3

UK s'est interrogée sur la praticabilité de cette disposition.

Article 10 : Renvoi d'appels

La Commission a rappelé que cet article a été introduit suite aux souhaits du Parlement européen.

Les délégations D, IRL et UK se sont interrogées sur l'opportunité de cet article.

B, de son côté, a suggéré que le texte de cet article soit formulé d'une manière plus correcte.
Compte tenu que ces remarques la Commission a été invitée à clarifier son texte.

**Article 11 : Annuaires**

P s'est félicitée de ce que, aux termes de la proposition de la Commission, l'abonné ait le droit d'obtenir gratuitement de ne pas figurer dans l'annuaire.

Pour F cette question devrait relever de la subsidiarité.

B suggère de combiner cet article avec l'article 7 paragraphe 2 de la proposition initiale.

UK s'est interrogée sur la notion d"'annuaires".

NL a indiqué que la version néerlandaise est incorrecte.
OUTCOME OF PROCEEDINGS

of: Working Party on Telecommunications

on: 1 September 1995

No. prev. doc.: 9273/95 ECO 140
No. Cion prop.: 7966/94 ECO 156


1. The Working Party completed the first reading of the above proposal at its meeting on 1 September 1995.

   Delegations' main comments concerning Article 12 and the following Articles are annexed to this document (see 9273/95 for the first eleven Articles).

2. Following the first reading and after asking delegations which so wished to send any
additional comments (1) to the Council General Secretariat, the Presidency expressed its intention of submitting shortly a compromise text for pursuing the discussions on this Directive.

(1) A/D and IRL pointed out that they wanted to raise new points, in particular with regard to the text examined at the previous meeting. (IRL stated in particular that its misgivings concerned deceased persons and Article 9(1)(b)).
Examination of Article 12 and the following Articles

Article 12: Surveillance of communications

Several delegations wondered about the actual principle of this Article given that it deals with a question covered by the Treaty's provisions on cooperation in the fields of justice and home affairs (Third Pillar).

DK and NL were concerned about the excessive burden which, in their opinion, was likely to be placed on Member States if those provisions were applicable to analogue networks. (The Commission pointed out that this Directive was applicable to analogue networks only where technically possible.)

A and B wanted telephone-tapping to be authorized only by judicial authorities.

With regard to paragraph 2, E/FIN/NL and UK feared implementing difficulties in the case of a number of commercial activities (UK mentioned stockbroking in particular); F wondered to what extent that paragraph was compatible with the objective of free movement of the equipment concerned; A/D and E pointed out moreover that the reference to storage on tape was too restrictive.

With regard to paragraph 3, DK suggested referring to Article 9 as a whole, IRL having suggested the following amendment:

"Paragraph 2 does not apply in cases of authorized listening and recording of communications in accordance with paragraph 1 or in cases covered by Article 9(1)".
Article 13: Unsolicited calls

DK/F/IRL/NL/I/P and UK wondered about the desirability of retaining such an Article in this Directive which seems to duplicate the provisions of the draft Directive on distance selling; UK, supported by S, wanted at least calls made for research purposes to be excluded. (1)

A/D/FIN and the Commission considered that this was an essential provision which had to stand, the Commission emphasizing that its scope was wider than the text of the draft Directive on distance selling.

Article 14: Technical features and standardization

D, pointing out that Germany applied more stringent standards concerning personal data protection, asked the Commission to define the scope of the planned standards; that delegation wanted to know in particular whether those standards would be minimal and would therefore enable the Member States to apply more rigorous standards within their territory if necessary.

The Commission undertook to supply the details requested at the next meeting to be held on this Directive.

Article 15: Technical application and modification

Most delegations had considerable reservations concerning this provision.

(1) There are differences between the language versions; in particular the term "research" is not included in all the versions.
Article 16: Judicial remedy and sanctions

F suggested aligning the text of this Article on the corresponding provisions of the general Directive (Articles 22 et seq.). That suggestion was welcomed by most delegations.

Article 17: Working Party on the Protection of individuals with regard to the processing of personal data

B and I expressed misgivings about providing in paragraph 2 that the Working Party will be specifically constituted for the purposes of this Directive.

Article 18: Procedure (committee procedure)

DK/D/E/F/P and UK stated that they were in favour of a type III(b) Regulatory Committee procedure.

B and L did not want to depart from the solution adopted for the general Directive, namely a type II(b) procedure.

IRL expressly reserved its position.


The Working Party agreed to leave in abeyance at this stage the date of entry into force of the Directive; it was pointed out in this context that the date could not in any case be earlier than that of the entry into force of the general Directive (24 July 1998).
Other business

UK wanted a provision equivalent to Article 13 of the general Directive to be introduced, enabling Member States to provide for exceptions and restrictions on the obligations laid down in this Directive.
OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Data Protection)
on: 22 and 23 January 1996

No. Cion prop.: 7966/94 ECO 156

Subject: Amended proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the context of digital telecommunications networks

In accordance with the conclusions of the Permanent Representatives Committee on 10 January 1996, the Working Party on Economic Questions (Data Protection) (1) continued examining the above proposal with the aim, announced by the Presidency, of adoption of a common position at the Telecommunications Council in May.

(1) Coreper agreed inter alia that the experts on the Working Party on Telecommunications would be kept informed of progress and could, if necessary, be asked to attend joint meetings.
The Working Party was able to make a complete reading of the draft Directive submitted by the Spanish Presidency in November 1995 (Working document No 17/95) (\(^2\)).

I. General remarks

- DK, E and FIN still had doubts about the need for this Directive.

- Several delegations wanted the Directive to be in the most simplified form possible and to comply fully with the principle of subsidiarity. The Chairman pointed out that the amended proposal had already been extensively recast to conform to that principle.

- One delegation (F) feared that the text under examination did not look far enough ahead and in particular did not take sufficient account of the new challenges of the multimedia society. (The Commission representative responded that multimedia applications were within the scope of the Directive: point-to-point communications were covered, multipoints not.)

- Many delegations called for clarification of the links between this Directive and the general Directive. The Presidency said that it intended to include an Article to that

\(^2\) Throughout discussion of the various Articles, the Presidency put forward the comments of the Data Protection Commissioners on the amended proposal.
effect (1) which would state in particular that this Directive did not amend the general Directive and would allow all the other references to the general Directive to be deleted.

II. **Main comments on the Articles**

These comments are summarized below:

**Article 1: Objective of the Directive**

As regards the scope of the Directive, the following points were made:

- D/E and NL were very reluctant to include analogue networks, in view of the cost. (For DK mobile analogue networks should in any case be excluded from the Directive.)

  Other delegations, while sharing these concerns, could agree that the Directive should extend to such networks, subject to specific conditions (see below, discussion of Article 3(3)).

- The Commission pressed for an across-the-board approach covering analogue and digital networks, stressing that in practice it was difficult to distinguish between the two;

- DK wanted the Directive not to cover natural persons; D and A, however, insisted

(1) At the end of the meeting the Italian Presidency announced that in early February it would be submitting a document to serve as a basis for discussion at the Working Party’s next meeting, scheduled for 19 and 20 February.
that they be included in the scope.

A number of suggestions were put forward for the wording of this Article:

– A proposed referring to free movement of data as well as free movement of equipment;

– D wanted a reference to the confidentiality of communications;

– UK suggested that in the second paragraph (line 2) "complete" be replaced by "complement" and that a clearer word be used than "specify" (for example "amplify").

Concluding discussion of this Article, the Chairman said that he would try to align the text on Article 1 of the general Directive.

Article 2: Definitions

DK/ E/F/IRL and I urged that in general the definitions used in this Directive be consistent with those in other Community texts on telecommunications.

Specific comments were made on some definitions:

– Subscriber: A wanted a more precise definition.

– Public network: D and A thought that the definition should make clearer the distinction between public and private networks. (The Presidency pointed out that private networks were covered by the general Directive.)
– Public telecommunications service: D and A called for the inclusion of radio and television broadcasting in the Directive; E and F opposed that request.

– The Chairman wondered whether there should not be a definition of "provider", which appeared several times in the text.

Article 3: Services concerned

DK/NL and UK wanted "digital" to be reinstated before "mobile networks" in paragraph 1.

DK and UK called for the reinstatement of paragraph 3 of the amended proposal. They were supported by E, which also wanted "and economically viable" to be added. D and I accepted the inclusion of analogue networks in the Directive but thought that they should be the subject of derogations.

Article 4: Security

UK, with the support of E/I and L, suggested replacing "encryption facilities" (penultimate line) with "alternative remedies", arguing that there were other possibilities, such as rerouting and numeric signature; IRL suggested "where technically feasible"; NL/FIN and S suggested waiving the obligation to offer encryption facilities and simply informing users of the risks.

DK/E/F/NL/FIN/S and UK wanted to delete the end of the sentence (from "free of charge or at no more"); I suggested the expression "cost-oriented".
A and IRL were unclear about the division of responsibilities between the service provider and the network provider. (The Commission said that according to Community definitions "service" covered network provision.)

D asked what exactly was the point of these measures, while DK thought that the expression "state of the art" (lines 2 and 3) was too vague.

Concluding examination of Article 4, the Chairman pointed to the solution put forward in the Commissioners' document (end to end protection) and cited recital 47 in the general Directive in response to the concerns of A and IRL. He proposed acting on the suggestions concerning the latter part of the Article by introducing the concept of proportionality (taken from the general Directive).

**Article 5: Traffic and billing data**

These provisions prompted many requests for clarification, in particular

- A and D wanted to know whether billing data could be used for other ends. (The Commission said that according to the general Directive it could.)

- FIN raised the problem of conservation of data in the event of dispute, pending legal settlement of the matter;

- NL/IRL and UK wanted a clearer definition of the persons covered by paragraph 3 (in particular, did they include anti-fraud personnel?). IRL suggested that in line 4 "in charge of billing or traffic management" be replaced by "handling billing, customer services and/or traffic management".
– **UK** raised the question of information for other telecommunications programmes;

– **I and UK** wondered whether it was advisable to cover anonymous data (paragraph 4).

**Article 6: Itemized billing**

Discussion of this Article revealed that most delegations were in favour of leaving subscribers the choice of whether or not to have an itemized bill.

Delegations differed on the provisions concerning non-identification of the calling line. The Chairman said that this was just an example, the main point being the obligation on Member States to safeguard privacy.

**Article 7: Calling-line identification**

**F** maintained a scrutiny reservation on the entire Article.

**B** wanted natural persons not to be authorized to eliminate calling-line identification, to preclude harassment of private individuals.

**DK**, supported by **FIN and P**, were opposed to making this a free service. (**P** suggested substituting "cost-oriented").

The following amendments were suggested to paragraph 1:

– replace "transmission" with "disclosure" (I);
– replace "of his/her subscriber number" with "to the call subscriber terminal" (IRL);

– replace "on a per-line basis" with "permanent basis" (NL/I).

On paragraph 2, S queried the practical application of (a), while D and F wanted (b) to be deleted; P thought that it was too vaguely worded.

There were doubts about paragraph 3 on the part of E, which referred to the multilateral negotiations in Geneva, and F, which asked how these provisions tied in with Article 25(2) of the general Directive.

GR proposed that the following be added to Article 7:

"1. Where calling-line identification presentation (CLIP) is offered ... subscriber number (Calling Line Identification Restriction: CLIR) for the purpose ...

2. (d) to eliminate the presentation of the actually called number to the calling party. (Connected Line Restriction: COLR)."

Article 8: Exceptions

Several delegations found paragraph 1 too restrictive. (IRL and UK proposed adding "or on specific request in conformity with law" to (b); in the same vein NL suggested "from the appropriate national authorities" and I "any judicial authority".)

UK thought that "on request" in paragraph 2 was unnecessary.
**Article 9: Call forwarding**

**DK** entered a scrutiny reservation on this Article.

It was asked whether this function was to be on the network or on the terminal. **IRL** proposed that the text state specifically "to the called subscriber terminal" instead of "by a third party". **E/I** and **FIN** thought that if this function was on the network it should be free.

**Article 10: Directories**

Several delegations (**IRL/L/NL** and **UK**) saw little point in offering subscribers the possibility of having their addresses withheld. There should be two choices: either to be included in the directory with identification or not to be included at all.

Several delegations (**A/D/GR/L** and **P**) raised the questions of the use of data in directories for commercial ends. The Chairman said that the Commissioners' document proposed that subscribers be able to have a symbol indicating a ban on such use placed against their entries in the directory.

**D** wondered about the possibility of mentioning the spouse or children of the subscriber.

**Article 11: Surveillance of communications**

**D/DK** and **S** had serious doubts about the practicability of paragraph 1. **E** and **NL** wanted "consent" reinstated in place of "prior knowledge".

**UK**, supported by **D/DK/E** and **F**, proposed deleting paragraph 2. **UK** suggested
incorporating in this Directive Article 3(2), Article 13(1) and recitals 13 and 16 of the general Directive.)

The Commission proposed, in response to a comment by the Presidency, that the notion of confidentiality be included in the title of the Article.

Article 12: Unsolicited calls

DK wondered whether this Article did not duplicate Article 10 of the Directive on distance selling.

E and L criticized the use of the term "direct marketing"; the Commission said that it was taken from the general Directive.

UK maintained a scrutiny reservation on "designated" (line 5).

Article 13: Technical features and standardization

No comments, apart from a reminder that Directive 91/263, referred to in paragraph 3, was the subject of a proposal recently submitted by the Commission relating to legislative consolidation of the rules in force on telecommunications terminal equipment and satellite earth station equipment (see 4278/96 of 15 January 1996).

Article 14: Technical application and modification

E suggested covering new market developments as well as new technical developments.
F/NL and UK asked about the extent of the powers conferred on the Commission by virtue of the type of Committee chosen. F entered a formal reservation on this point.

Article 15: Judicial remedy and sanctions

The Chairman said that this Article would be reviewed in the light of the new Article on the link with the general Directive.

Article 16: Working Party on the protection of individuals with regard to the processing of personal data

Two problems were raised in connection with this Article:

– that of the presence of experts from the telecommunications sector when the Working Party was specifically constituted for the purposes of this Directive (and the secondary matter of the relationship between this Working Party and the Committee set up under Article 31 of the general Directive) (A/F and GR);

– that of the powers of this Working Party to deal with aspects other than data protection in the strict sense, such as free movement of equipment (DK and E).

Article 17: Committee procedure

DK/E/P/S and UK were in favour of a IIIb Committee procedure; NL was opposed to a consultative committee, but had not yet decided between a IIIa and a IIIb Committee; IRL reserved its position.

Article 18: Entry into force

There was a consensus in favour of the same date as that set for the entry into force of the general Directive.
EUROPEAN UNION
THE COUNCIL

Brussels, 1 April 1996

6186/96

LIMITE

ECO 88
CODEC 188

OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Data Protection)
dated: 18/19 March 1996

No. prev. doc.: 4613/96 ECO 17 CODEC 42
No. Cion prop.: 7966/94 ECO 156

Subject: Modified 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks

Delegations will find hereafter in Annex I the text of the above-mentioned proposal, resulting from the deliberations of the Working Party on Economic Questions on 18 and 19 March 1996.

Annex II contains amendments to the text of the proposal suggested by the Presidency in the light of the latest discussions by the Working Party.
Draft Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks\(^{(1)}\)

\(^{(1)}\) P maintained a preference for the original title.
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof;

Having regard to the proposal from the Commission,

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

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data exhorts Member States to ensure the rights and freedom 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) Whereas currently in the European Community new advanced digital public telecommunications networks are emerging which give rise to specific requirements concerning the protection of personal data and privacy of the user;

(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;
(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas in the case of telecommunications networks, specific legal, regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of users and legitimate interests of subscribers, in particular with regard to the increasing risks connected with computerized storage and processing of personal data in such networks;

(7) Whereas several Member States have already adopted diverging provisions in this area; whereas a number of Member States are currently developing legislation which bears the risk to increase the existing differences;

(8) Whereas these divergent legal, regulatory, and technical provisions concerning the protection of personal data and privacy in the context of the implementation of telecommunications networks in the Community, in particular the Integrated Services Digital Network (ISDN) and digital mobile networks, create obstacles to the creation of an internal market for telecommunications in conformity with the objective set out in Article 8A of the Treaty; whereas the importance of these differences and the necessity to ensure the freedom of transborder telecommunications within the Community require specific harmonization at Community level; whereas the harmonisation envisaged is strictly limited, pursuant to the principle of subsidiarity, to the specific requirements which have arisen as a result of the introduction of new functionalities in telecommunications networks;

(8bis) Whereas these new functionalities include service such as interactive television and video on demand;

(9) Whereas in the telecommunications sector, 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 the individuals Directive 95/46/EC shall apply; whereas in particular pursuant to Article 13 of the said Directive, Member States can restrict the scope of those obligations and rights in certain circumstances; whereas Directive 95/46/EC shall apply to non-public telecommunication services;

6186/96 prk EN

6) P questioned what is exactly covered by "video on demand".
(10) Whereas the personal data processed to establish calls are highly sensitive, in particular in the case of digital mobile networks; whereas the storage of these data should be limited to the period strictly necessary for the provision of the service;

(11) Whereas currently diverging rules exist in the Member States with regard to the provision of itemized bills; whereas this Directive must provide for harmonization of the Member States rules concerning the privacy in the field of itemized billing in order to avoid obstacles to the development of transEuropean services;

(12) Whereas, it is necessary, as regards the calling line identification, to protect both the right of the calling party to remain anonymous and the privacy of the called party with regard to unidentified calls; whereas however, it is justified to override the elimination in specific exceptional cases;

(13) Whereas directories are widely distributed and publicly available; whereas the right to privacy requires that the subscriber himself is able to determine to which extent his personal data are published in a directory;

(14) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications;

(15) Whereas safeguards must be provided for the users against intrusion into their privacy by means of forwarded calls as well as unsolicited calls and telefaxes;

(16) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonized in order to be compatible with the implementation of the internal market;

(17) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(18) Whereas Member States, industries concerned and the European Community will have to cooperate in developing and manufacturing the technologies necessary for the implementation of this Directive; this cooperation will have to respect, in particular the competition rules of the Treaty;

(19) Whereas this Directive, in conformity with Article 3 of directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities, such as national security, which are not governed by Community law;
(20) Whereas the processing of personal data may not be used
to give telecommunications organizations any undue competitive
advantage over other service providers;

(21) Whereas 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 in Article 29 of
Directive 95/46/EC;

(22) Whereas it is useful to determine the details of
application of this Directive with the assistance of the
Committee composed of representatives of the Member States set
up in Article 31 of Directive 95/46/EC;

HAS ADOPTED THIS DIRECTIVE:

Article 1
Objective

1. This Directive provides for the harmonization 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 telecommunications
sector and to ensure the free movement of such data and of
telecommunications equipment and services in the Community. (1)

2. For the purposes mentioned in paragraph 1, the provisions
of this Directive particularise and complement Directive
95/46/EC of the European Parliament and of the Council on the
protection of individuals with regard to the processing of
personal data and the free movement of such data. (2)

3. This Directive shall not apply to the activities which fall
outside the scope of Community law, such as those provided for
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 activity relates to state security matters]) and the
activities of the State in areas of criminal law. (3)
The group accepted the new text as proposed by NL, subject to linguistic scrutiny.

In response to the wishes primarily of A, D and P which had called for the inclusion of "legal persons", the Cion proposed the following text for Article 1 §2:

"For the purposes mentioned in paragraph 1, the provisions of this Directive particularise Directive 95/46/EC and complement that Directive, in particular with regard to the legitimate interests of legal persons".

A number of delegations (B, ES, FIN, NL, UK) maintained a scrutiny reserve on this proposal and E maintained a reserve in respect of the inclusion of "legal persons" which it considered in contradiction with the general Directive on data protection.

The Presidency indicated it would present a new text which would clarify that the protection of certain legitimate interests of legal persons was a specific issue and did not impinge on the general Directive.

A clear majority of delegations were in favour of this new paragraph with the additional text in square brackets. D nevertheless maintained a scrutiny reserve.
Article 2
Definitions

In addition to the definitions given in Directive 95/46/EC for the purposes of this Directive:

a. 'subscriber' means any natural or legal person who or which is party to a contract with the provider of public telecommunications services for the supply of such services;

b. 'user' means any person using a public telecommunications service for private or business purposes without necessarily having subscribed to this service;

c. 'public telecommunications network' means the transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined network termination points by wire, by radio, by optical or by other electromagnetic means, which are used inter alia for the provision of public telecommunications services;

d. 'public telecommunications service' means a service whose provision consists wholly or partly in the transmission and/or routing of signals on telecommunications networks and which is available to the public, with the exception of radio and television broadcasting.

Article 3
Services concerned

This Directive applies to the processing of personal data in connection with the provision of public telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

Article 4
Security

1. The provider of a public telecommunications system must take appropriate technical and organisational measures to safeguard network security. Having regard to the state of the art and the costs of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
As three of these definitions also featured in the ONP interconnection Directive, the group agreed to postpone examination of the definitions until a common position was reached on the interconnection Directive and further progress was made on the common set of definitions currently under examination by the telecommunications working group (doc. 5151/96) with a view to either repeating the definitions adopted or making a reference to them in this text.

Expressed difficulties with definitions for "subscriber" in relation to the inclusion of "legal person" and with "user" where they wanted to refer to "physical person". ES on the other hand, pointed out that the definition of "user" in other telecoms texts included "legal persons".

 indicated their conditional acceptance of the Presidency text. ES, DK, NL, P and S showed some flexibility but maintained a scrutiny reserve on Article 3 at this stage, preferring that it should read "in public telecommunications digital networks in the Community", and should specify that the Directive was applicable to processing data in connection with services providing analogue networks where technically possible or where it did not involve disproportionate effort.

 in particular considered that the provider of the network rather than the service provider should be responsible for safeguarding security and proposed to add "and/or network" after "the provider of a public telecommunications service".

In response to these concerns, the at the suggestion of the UK, proposed to start paragraph 1 with:

"The network operator or, where appropriate, the provider of a public telecommunications service ...".

The Group undertook to further examine this latest proposal.

In addition, maintained its proposal to include a reference to the security standards elaborated by SOGIS.
2. In case of a particular risk of a breach of the security of the network, the provider of a public telecommunications service must inform the subscribers concerning such risk and about the possible remedies, including the costs involved.\(^{(7)}\)

Article 5

Traffic and Billing Data

1. Traffic data relating to users and subscribers processed to establish calls and stored by the provider of a public telecommunications network and/or service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraph 2.\(^{(6)}\)

2. For the purposes of subscriber billing and interconnection payments, data containing the number or identification of the subscriber station, the address of the subscriber and the type of station, the total number of units to be charged for the accounting period, the called subscriber number, the type, start time and duration of the calls made and/or the data volume transmitted as well as other information concerning payment such as advance payment, payment by instalments, disconnection and reminders, 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 may be pursued. For the purpose of marketing its own services, the provider of a public telecommunications service may process such data, if the subscriber has [...] given his consent.\(^{(8)}\)

3. Processing of traffic and billing data must be restricted to the personnel of the providers of the public telecommunications networks and/or services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own services and it must be restricted to what is necessary for the purposes of such activities.\(^{(9)}\)

4. Paragraphs 1, 2 and 3 apply without prejudice to the possibility for the competent authorities to be informed of billing or traffic data in accordance with applicable legislation [in view of settling disputes].\(^{(10)}\)
The vast majority of delegations accepted the new text for paragraph 2, LUX nevertheless maintaining a substantial reserve and E. and the Cion scrutiny reserves.

Scrutiny reserve by F and P, who prefer to delete "users" from paragraph 1.

F in particular maintained its view that the list of personnel indicated in this paragraph was too restrictive and suggested deletion of the list unless it could be shown that it was necessary to include it. D, FIN and IRL indicated their preference for the last clause of paragraph 2 to read: "if the subscriber has not registered his disagreement".

LUX expressed some hesitancy about the term "interconnection payments" and agreed to look for clearer terminology. G called for a definition of "subscriber station".

D also preferred the text to specify that the service provider could transmit data to various bodies, such as the police, as long as it was in the interest of public security.

A and G noted their preference for the emphasis to be on the task involved rather than the people carrying out the task, A also would wish the text to specify there was a duty to keep data confidential.

The UK request to delete "in view of settling disputes" was supported by a number of delegations, but opposed by the Cion who as an alternative solution, proposed adding Article 5 to the list of exemptions in the proposed new Article 15(2). A and LUX indicated the need to clarify the kind of disputes referred to in paragraph 4, with A proposing to add "relating to billing" at the end of this paragraph.
Article 6
Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.

2. Where an itemized bill is produced, Member States shall ensure that the privacy of calling users and called subscribers is preserved.\(^{(12)}\)

Article 7
Calling and connected line identification\(^{(13)}\)

1. Where calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge to eliminate the presentation of the calling-line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.\(^{(14)}\)

2. Where calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge:

   (a) to eliminate the identification of all incoming calls;

   (b) to prevent the access to the identification of incoming calls by unauthorized persons;

   (c) to reject incoming calls where the calling line identification has been eliminated by the calling user.\(^{(15)}\)

3. Where connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge to eliminate the presentation of the connected line identification to the calling party.\(^{(16)}\)

4. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2 and 3 shall also apply to incoming calls originating in third countries.

5. Member States shall ensure that where calling-line identification and/or connected line is offered, the providers of public telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2 and 3.
A number of delegations (B, DK, FIN, F, IRL, S, UK) favoured deleting 6.2, some pointing out that it was technically impossible to ensure privacy if a fully-itemised bill was produced. A, D, ES, and P indicated that they could accept the Presidency proposal to delete the example of omitting the last 3 or 4 digits from this article and place it in a recital and FIN indicated that it could accept a more flexible version of paragraph 2.

ES and F maintained a scrutiny reserve on Article 7.

The President is prepared to add in this article a similar provision as Article 4(3). He will also present an addition specifying what kind of calling identification is intended for the purpose of this Directive (CLIP).

F and S maintained two reserves on this paragraph. A, UK and FIN requested deletion of "free of charge" (IRL suggesting "cost oriented"); P asked to replace in second line, "subscriber" by "users".

The President concluded that he will present a new formulation using a more flexible and general terminology.

P requested to replace "calling party" by "calling user".
Article 8
Exceptions

1. Member States shall ensure that the provider of a public telecommunications service and/or network may override the elimination of the calling-line identification:

(a) for a limited period of time, in exceptional cases upon application of a subscriber requesting the tracing of malicious or obscene calls; in this case, the data containing the identification of the calling subscriber will be stored by the provider of a public telecommunications service and be made available in accordance with internal law;

(b) 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 answering such calls.

Article 9
Call Forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to prevent and/or stop automatic forwarding by a third party to the subscriber's terminal.
Delegations welcomed the intention of the President to redraft this article in order to refer to the national procedures concerning the modalities and to take better account of Article 13 of the General Directive.

E suggested redrafting sub-paragraph (a) as follows:

"when a subscriber requests the tracing of malicious or obscene calls, and for the period strictly necessary to achieve this objective, the data containing the identification of the caller will be stored by ... internal law".

A requested replacing, in first line, in "exceptional cases" by "individual cases"; IRL requested to add after "internal law" the words "and/or national procedures". Note also request by NL to add to recital 19 the following text:

"For example, Member States shall ensure that the provider of a public telecommunications service shall override the elimination of the calling line identification upon specific decision from a judicial authority made in conformity with national legislation for the purpose of prevention or detention of criminal offences or security of the state."

UK indicated its preference for previous formulation.

As several delegations (DK, P, S, UK in particular) expressed reservations about the technical feasibility of preventing automatic forwarding by a third party, the group agreed to reflect further on this point.

D was concerned to ensure that the calling party was informed if a call was forwarded and proposed to add the following sentence:

"If a call is forwarded, it must be ensured that the calling party is informed of this."

ES and P reacted favourably to this addition, but the Cion has indicated a reserve in this respect.

ES proposed to refer to forwarding to "a subscriber's network termination point".

---

6186/96 prk EN
Article 10
Directories of subscribers

Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services, should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from the directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted [entirely or] in part and not to have a reference revealing his or her sex.\(^{(21)}\)

Article 11
Confidentiality of communications\(^{(22)}\)

1. Member States shall prohibit the disclosure by the calling and/or called users to anybody but the said users of the content of their telephone calls, or the storage of such content, without the prior knowledge of the users concerned.\(^{(23)}\)

2. Member States shall take appropriate measures to ensure that:

(a) access to the content of telephone calls by providers and subscribers who are not users may only be allowed with the consent of the users concerned;

(b) listening or tapping devices or other means of interception or surveillance of communications by third parties are applied only subject to authorization by the competent authorities in conformity with national legislation.

3. Paragraph 1 does not apply in cases referred to in Article 8.\(^{(24)}\)
A number of delegations maintained their reserves on this article:

- **F and D**: scrutiny reserve on the right to indicate that personal data cannot be used for direct marketing;

- **NL**: reserve on the right for the subscriber to have his address omitted entirely or in part. The IRL request to delete "entirely or" was supported by the Presidency;

- **F**: reserve on the right to be omitted from the directory "free of charge".

In addition, UK expressed some concerns about the application of the Directive to existing directories and A queried the link between Articles 10 and 12.

**E** maintained a general reserve on this article and **DK, S and UK** also expressed concern about the difficulties transposing it into national law. (UK could however accept paragraph 2).

D and P considered that the question of confidentiality should feature at the beginning of the Directive.

The group undertook to reflect further with respect to the link to the General Directive and on the basis of:

- the Presidency proposal: "Member States shall prohibit the listening of the content of telephone calls by persons other than calling or called users or storage of such content, without prior knowledge of the users concerned."

- the D proposal: "Member States shall ensure the confidentiality of telecommunications via national regulations." (ES and P) gave favourable indications for this approach).

IRL (supported by S) reiterated its proposal to redraft paragraph 3 as follows:

"Recording and storage of call content may be made without a caller's prior consent by organisations dealing with emergency calls and recognised as such as a Member State."
Article 12
Unsolicited calls

1. Notwithstanding the provisions of Directive .../... on the protection of consumers in respect of contracts negotiated at a distance (distance selling), Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing are not allowed without the consent of the subscribers concerned or in respect of subscribers who [notified to a body designated by the Member State or to the calling subscriber that they do not wish to receive these calls].

2. The use of automatic call devices for transmitting pre-recorded voice, telefax or other messages for purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

Article 13
Technical features and standardization

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council Directive 83/189/EEC which lays down a procedure for the provision of information in the field of technical standards and regulations.

UK and Cion maintained positive scrutiny reserves on the new text inserted at the suggestion of D.

Scrubiny reserve by DK and F who prefer deletion of this article or at least for it to be aligned further with Article 10 of the distance selling Directive, particularly in respect of a "body designated by the Member State". In response, the Presidency undertook to reflect further on the possibility of deleting the text in square brackets.

The UK also maintained a reserve in respect of paragraph 1 applying to legal persons, as they consider a company should not be able to refuse direct marketing.

Waiting reserve of A on paragraph 1; ES asked for clarification on whether paragraph 2 applied to networks or terminals.

The Cion undertook to provide answers to A and ES queries and announced that the forthcoming Directive on terminal equipment would consider data protection as an "essential requirement".
Article 14
Implementing measures

Implementing measures necessary to adapt this Directive to technical developments or to new services on offer shall be determined by the Commission in accordance with the procedure laid down in Article 15, paragraph 3.

Article 15
Extension of the scope of application of certain provisions of directive 95/46/EC

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

2. The Working Party on the Protection of individuals with regard to the processing of personal data established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the above-mentioned Directive also with regard to the protection of fundamental rights and freedoms, including the right to privacy, which is the subject of this Directive.

3. The Commission shall be assisted by the Committee established by Article 31 of Directive 95/46/EC which for the purposes of this Directive shall act according to the procedure mentioned therein.

Article 16
Implementation of the Directive

1. The Member States shall bring into force the laws, regulations, and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.

When Member States adopt these provisions, these shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.
A number of delegations (DK, ES, F, I, P, UK) expressed some concern that the scope of this article seemed to go beyond technical adaptation, with some suggesting that the articles likely to include adaptation should be specified.

Certain delegations (ES, F, NL, UK) indicated that their acceptance of such an article would be on the proviso that the committee procedure of Article 15, paragraph 3 was a Regulatory Committee type IIIb, with the Committee convening meetings of the working party specifically on telecommunications issues.

Several delegations (in particular DK and UK) considered the title of "Implementary measures" to be confusing and proposed returning to something along the lines of the Commission's original title of "Technical adaptation and modification".

Para. 1
F maintained a scrutiny reserve on paragraph 1 (which modified the scope of the general Directive in relation to legal persons).

Para. 2
In response to concerns of F and UK in particular, the Presidency proposed to add after "fundamental rights and freedoms", "in the telecommunications sector, in particular the right to privacy".

Para. 3
Delegations reiterated their positions on Article 14 with regard to the committee procedure and in particular insisted that the working party should hold specific meetings on telecoms issues involving the relevant telecoms experts. The Cion undertook to clarify this point in paragraph 2.

Cion maintained a reserve on Articles 14 and 15 in respect of a change to the committee procedure proposed (IIib).
This Directive is addressed to the Member States.
Modified 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 telecommunications sector, in particular in the Integrated Digital Network (ISDN) and in the public digital mobile networks.
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission,

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

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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) Whereas currently in the European Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;

(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas in the case of telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons in the telecommunications sector, must be harmonised in order to avoid obstacles to
the internal market for telecommunications in conformity with the objective set out in Article 8A of the Treaty; whereas the harmonisation pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new trans-European digital telecommunications services and networks will not be hindered;

(8) Whereas these new services include interactive television and video on demand;

(9) Whereas in the telecommunications sector, 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 the individual, Directive 95/46/EC shall apply; whereas Directive 95/46/EC shall apply to non-public telecommunications services;

(10) Whereas this Directive, in conformity with Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law;

(11) Whereas subscribers of a telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of the said Directive 95/46/EC to the protection of the legitimate interests of legal persons;

(12) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern their freedom of correspondence; whereas 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; whereas any further processing which the provider of the public telecommunications service may want to perform for the marketing of its own services may only be allowed if the subscriber has agreed to this;

(13) Whereas the introduction of itemised bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; at the same time it may jeopardise the privacy of the users of telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to telecommunications services;

(14) Whereas 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; whereas it is justified to override the elimination of CLI presentation in exceptional cases; whereas certain subscribers, in particular helplines and similar organisations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right 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; whereas the providers of public telecommunications services must inform their subscribers about the existence of calling and connected line identification in the network and about all services which are offered on the basis of calling and connected line identification.
and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use:

(15) Whereas directories are widely distributed and publicly available; whereas the right to privacy requires that the subscriber himself is able to determine to which extent his personal data are published in a directory;

(16) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications;

(17) Whereas safeguards must be provided for the users against intrusion into their privacy by means of forwarded calls as well as unsolicited calls and telefaxes;

(18) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(19) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(20) Whereas Member States, industries concerned and the European Community will have to cooperate in developing and manufacturing the technologies necessary for the implementation of this Directive; this cooperation will have to respect in particular the competition rules of the Treaty;

(21) Whereas 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 public telecommunications service may override the elimination of the presentation of calling line identification upon specific decision from a judicial authority made in conformity with national legislation for the purpose of prevention or detection of criminal offences or State security;

(22) Whereas 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 in Article 29 of Directive 95/46/EC;

(23) Whereas it is useful to determine the details of application of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC;

HAVE ADOPTED THIS DIRECTIVE:
Article 1
(Object and scope)

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularize and complement Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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 the activities which fall outside the scope of Community law, such as those provided for 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)

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) 'subscriber' means any natural or legal person who or which is party to a contract with the provider of public telecommunications services for the supply of such services;

(b) 'user' means any natural person using a public telecommunications service for private or business purposes without necessarily having subscribed to this service;

(c) 'public telecommunications network' means the transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined network termination points by wire, by radio, by optical or by other electromagnetic means, which are used inter alia for the provision of public telecommunications services;

(d) 'public telecommunications service' means a service whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks and which is available to the public, with the exception of radio-and television broadcasting.
Article 3
(Services concerned)

This Directive applies to the processing of personal data in connection with the provision of public telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

Article 4
(Security)

1. The provider of a public telecommunications service must take appropriate technical and organizational measures to safeguard security of its services if necessary in conjunction with the provider of the public telecommunications 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 public telecommunications service must inform the subscribers concerning such risk and the possible remedies, including the costs involved.

Article 5
(Traffic and billing data)

1. Traffic data relating to users and subscribers processed to establish calls and stored by the provider of a public telecommunications network and/or service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraph 2.

2. For the purpose of subscriber billing and interconnection payments, data containing the number or identification of the subscriber station, the address of the subscriber and the type of station, the total number of units to be charged for the accounting period, the called subscriber number, the type, start time, and duration of the calls made and/or the data volume transmitted as well as other information concerning payment such as advance payment, payment by instalments, disconnection and reminders, 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 may be pursued. For the purpose of marketing its own services, the provider of a public telecommunications service may process such data, if the subscriber has given his consent.

3. Processing of traffic and billing data must be restricted to the personnel of providers of the public telecommunications networks and/or services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own services and it must be restricted to what is necessary for the purposes of such activities.
4. Paragraphs 1, 2 and 3 apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation (in view of settling interconnection disputes).

Article 6  
(Itemized billing)

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative modalities for communications are available to such users and subscribers.

Article 7  
(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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge

(a) to prevent the presentation of the calling line identification of incoming calls;

(b) to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

3. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

4. The provisions set out in paragraphs 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2 and 3 shall also apply to incoming calls originating in third countries.

5. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of public telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2 and 3.
Article 8
(Exceptions)

Member States shall ensure that the provider of a public telecommunications service may override the elimination of presentation of the calling line identification:

(a) on a temporary basis, upon application of a subscriber requesting the tracing of malicious calls; in this case, the data containing the identification of the calling subscriber will be stored by the provider of a public telecommunications service and/or network and be made available in accordance with national law;

(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 9
(Call forwarding)

1. Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to (prevent and/or) stop automatic call forwarding by a third party to the subscriber’s network termination point.

[2. The calling subscriber must be informed automatically during the establishment of the connection that the call is being forwarded to a third party.]

Article 10
(Directories of subscribers)

Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from the directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted [entirely or in part] and not to have a reference revealing his or her sex.

Article 11
(Confidentiality of communications)

Member States shall ensure the confidentiality of communications. In particular, they shall prohibit listening, tapping, storage or other means of interception or surveillance of communications by others than the users, without the consent of the users concerned.
Article 12
(Unsolicited calls)

1. Notwithstanding the provisions of Directive .../... on the protection of consumers in respect of contracts negotiated at a distance (distance selling), Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, as determined by national legislation.

2. The use of automatic call devices for transmitting pre-recorded voice, teletext or other messages for purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

Article 13
(Technical features and standardization)

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council Directive 83/189/EEC which lays down a procedure for the provision of information in the field of technical standards and regulations.


Article 14
(Implementing measures)

Implementing measures necessary to adapt Articles 4, 5, 7 and 9 of this Directive to technical developments or to new services on offer shall be determined by the Commission in accordance with the procedure laid down in as per Article 15, para. 43.

* An alternative text may be found by reference to Art. 29 of Directive 95/62/EC of the European Parliament and of the Council of 13 December 1995 on the application of open network provisions (ONP) to voice telephony.
Article 15

(Extension of the scope of application of certain provisions of Directive 95/46/EC)

1. Exemptions and restrictions mentioned by Article 13 of Directive 95/46/EC may be extended with regard to rights and obligations provided for in Articles 5, 7 para. 1 and 3, and 11 of this 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 established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the above-mentioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission shall be assisted by the Committee established by Article 31 of Directive 95/46/EC according to the procedure mentioned therein. It shall be convened specifically for the subjects covered by this Directive.

Article 16

(Implementation of the Directive)

1. The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.

When Member States adopt these provisions, those shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By derogation to the last sentence of Article 5.2, consent is not required with respect to processing already under way on the date the provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 10 shall not apply to editions of directories which have been published before the provisions adopted pursuant to this Directive enter into force.

4. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.

Article 17

(Addressees)

This Directive is addressed to the Member States.
OUTCOME OF PROCEEDINGS

from: Working Party on Economic Questions (Data Protection)
dated: 15/16 April 1996

No. prev. doc.: 6186/96 ECO 88 CODEC 188
No. Cion prop.: 7966/94 ECO 156

Subject: Modified 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks

Delegations will find hereafter the text of the above-mentioned Directive as it stands at the conclusion of the Working Party's deliberations.¹)

(1) See also report of the Working Party to COREPER doc. 6600/96 ECO 111 CODEC 226.
DRAFT DIRECTIVE
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR, IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND IN THE PUBLIC DIGITAL MOBILE NETWORKS(1)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission,

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

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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) Whereas currently in the European Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand,

(1) Most delegations maintained a general linguistic reservation.
interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;

(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonised in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8A of the Treaty; whereas the harmonisation pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks in more than one Member State will not be hindered;

(8) Whereas these new services include interactive television and video on demand;
(9) Whereas in the telecommunications sector, 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 the individual, Directive 95/46/EC shall apply; whereas Directive 95/46/EC shall apply to non publicly available telecommunication services;

(10) Whereas this Directive, in conformity with article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law;¹)

(11) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons;²) whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of the said Directive 95/46/EC to the protection of the legitimate interests of legal persons;

(12) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications;³)

(13) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern their right to respect for correspondence; whereas 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; whereas any further

(1) UK requested to add the following recital:

"Whereas it remains the responsibility of Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications;"

(2) Reservation by F.

(3) LUX requested to insert a recital related to Article 4 on security.

(4) UK requested to add the following words "by means of public telecommunications network and publicly available telecommunications service".
processing which the provider of the publicly available telecommunication service may want to perform for the marketing of its own telecommunications 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 telecommunications service about the types of further processing he intends to perform;

(14) Whereas the introduction of itemised bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider, at the same time it may jeopardise the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemised bills;

(15) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in exceptional cases; whereas certain subscribers, in particular helplines and similar organisations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right 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; whereas the providers of publicly available telecommunications services must inform their subscribers about the existence of calling and connected line identification in the network and about all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;
(16) Whereas directories are widely distributed and publicly available; whereas the right to privacy requires that the subscriber himself is able to determine to which extent his personal data are published in a directory;

(17) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas in such cases it must be possible for the subscriber to stop the forwarded calls being passed on to his terminal by simple request to the provider of the publicly available telecommunications service;

(18) Whereas safeguards must be provided for the users against intrusion into their privacy by means of unsolicited calls and telefaxes;

(19) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(20) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(21) Whereas Member States, industries concerned and the European Community will have to cooperate in developing and manufacturing the technologies necessary for the implementation of this Directive; this cooperation will have to respect in particular the competition rules of the Treaty;(1)

(22) Whereas 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

---

(1) Reservation by UK.
telecommunications 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 State security;

(23) Whereas 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 in Article 29 of Directive 95/46/EC;(1)

(24) Whereas given the technological developments in the telecommunications sector and the attendant evolution of the services on offer, it will be necessary to determine the technical modalities necessary for the application of certain provisions of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;(2)

HAVE ADOPTED THIS DIRECTIVE:

(1) UK requested to specify that it is useful for Member States to encourage the attendance in the Working Party of representatives of the NRA.

(2) New recital proposed by the President in relation to Article 14.
Article 1

(Object and scope)

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.\(^{(1)}\)

3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for 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.

\(^{(1)}\) Reservations by F, NL and UK on last two lines of this §.
Article 2

(Definitions)

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) 'subscriber' means any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;

(b) 'user' means any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) 'public telecommunications network' means transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) 'telecommunications service' means services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio-and television broadcasting.
Article 3
(Services concerned)

This Directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.\(^{(1)}\)

Article 4
(Security)

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.\(^{(2)}\)

---

(1) Scrutiny reserve by ES.
(2) Reservations by LUX and Cion on this §.
Article 5
(Confidentiality of the communications)

Member States shall ensure the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned.\(^{(2)}\)

Article 6
(Traffic and billing data)

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2 and 3.

2. For the purpose of subscriber billing and interconnection payments, data containing the number or identification of the subscriber station, the address of the subscriber and the type of station, the total number of units to be charged for the

---

(1) The group agreed to place Article 12 of the modified proposal after Article 4; consequently the following articles have been renumbered.

(2) Reservations by DK, F and NL on this provision. ES and UK requested to add, in 4th line, the word "unauthorized" after "they shall prohibit".

6599/96 prk EN
- 11 -
accounting period, the called subscriber number, the type, start time, and duration of the calls made and/or the data volume transmitted as well as other information concerning payment such as advance payment, payment by instalments, disconnection and reminders, 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 may be pursued.  

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection disputes.  

---

(1) Reservation by E.
(2) Reservation by F on the words "in particular interconnection disputes".
Article 7

(Itemized billing) (*)

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge. (1)

(*) See also recital no 14.
(**) See also recital no 15.
(1) Reservation by F, UK, FIN and S and scrutiny reserve by NL and IRL on the words "free of charge".
(a) to prevent the presentation of the calling line identification of incoming calls;

(b) to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

3. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

4. The provisions set out in paragraphs 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2 and 3 shall also apply to incoming calls originating in third countries.

5. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2 and 3.

---

(1) Reservation by FR on subparagraph (b) and scrutiny reserve by UK.
Article 9
(Exceptions)

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10
(Automatic call forwarding)

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

(1) D requested to add the following provision: "The calling subscriber must be informed automatically during the establishment of the connection that the call is being forwarded to a third party".
Article 11

(Directories of subscribers)

Personal data contained in printed or electronic directories\(^1\) of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge,\(^2\) to be omitted from the directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing,\(^3\) to have his or her address omitted in part\(^4\) and not to have a reference revealing his or her sex.

---

(1) \(\mathbf{D}\) requested that a subscriber should be able to distinguish between permission for printed and electronic directories.

(2) Reservation by \(\mathbf{F}\) on "free of charge".

(3) Reservation by \(\mathbf{D}\) on the sentence "to indicate that his or her personal data may not be used for the purpose of direct marketing".

(4) \(\mathbf{NL}, \mathbf{UK}\) requested to delete "to have his or her address omitted in part".
Article 12
(Unsolicited calls)(1)

1. Notwithstanding the provisions of Directive .../... on the protection of consumers in respect of contracts negotiated at a distance (distance selling), Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, as determined by national legislation.

2. The use of automatic call devices for transmitting pre-recorded voice, telefax or other messages for purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

(1) Independantely of the respective scope of the two directives, the group agreed in principle to align this text on Article 10 of the Directive "Distance-selling".

(Please note that Article 10 of the Common Position on this Directive reads as follows:

"1. Use by a supplier of the following means requires the prior consent of the consumer:

- automated calling system without human intervention (automatic calling machine)

- facsimile machine (fax).

2. Member States shall ensure that means of communication at a distance, other than those referred to in paragraph 1, which allow individual communications, may be used only where there is no clear objection from the consumer.")
Article 13

(Technical features and standardization)

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council Directive 83/189/EEC which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications.
Article 14

(Technical modalities)(1)

Technical modalities necessary to apply Articles 4, 6, 8 and 10 of this Directive in view of technological developments or new services on offer shall be determined by the Commission in accordance with the procedure as per Article 15, para. 4.

Article 15

(Extension of the scope of application of certain provisions of Directive 95/46/EC)

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and 8, para. 1 and 3, when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, as referred to in Article 13 para. 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks

(1) See report of the group to COREPER doc. 6600/96 ECO 111 CODEC 226.
laid down in Article 30 of the above-mentioned Directive also 
with regard to the protection of fundamental rights and 
freedoms and of legitimate interests\(^{(1)}\) in the 
telecommunications sector, which is the subject of this 
Directive.

4. The Commission shall be assisted by the Committee 
established by Article 31 of Directive 95/46/EC according to 
the procedure mentioned therein. It shall be convened 
specifically for the subjects covered by this Directive.\(^{(2)}\)

**Article 16**

*(Implementation of the Directive)*

1. The Member States shall bring into force the laws, 
regulations and administrative provisions necessary for them to 
comply with this Directive by 24 October 1998 at the latest.

When Member States adopt these provisions, these shall 
contain a reference to this Directive or shall be accompanied 
by such a reference at the time of their official publication. 
The procedure for such reference shall be adopted by Member 
States.

2. By derogation to the last sentence of Article 6.2, consent is 
not required with respect to processing already under way on 
the date the national provisions adopted pursuant to this 
Directive enter into force. In those cases the subscribers shall

\(^{(1)}\) Reservation by F.

\(^{(2)}\) Reservations by ES, DK, NL, P, UK, S and 
Cion.
be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.

**Article 17**

(Addressees)

This Directive is addressed to the Member States.
ADDENDUM to OUTCOME OF PROCEEDINGS

from: Working Party on Economic Questions (Data Protection)
dated: 15/16 April 1996

Subject: Modified 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks

In view of the future examination of this dossier by the Committee of Permanent Representatives, the following observations have been sent to the Secretariat:

- The Representative of the Commission maintains a legal scrutiny reservation on the solution agreed upon for Article 12;

- P confirms the following requests:

  - Article 5: add at the beginning of this article, after the words "Member States", "via national regulations";

  - Article 6§1: replace the words "traffic data relating to subscribers and users" by the following "traffic data containing personal data";

  - Article 7: specify that free calls should not be listed on the itemized billing.

- P and UK confirm their wish to see Article 15§1 deleted; P in addition maintains a reservation on Article 14.
I. INTRODUCTION

This proposal is intended to supplement the general Directive on the protection of personal data (Directive 95/46/EC of 24 October 1995), by applying the general principles of that Directive to the specific requirements of telecommunications networks.

The original proposal dating from July 1990 was amended by the Commission in October 1992 to take account of the Opinion of the European Parliament (delivered on 11 March 1992) and to apply the principle of subsidiarity.

In the Council the proceedings on this proposal did not really get underway until after the general Directive had been adopted, and were conducted in association with the participants in the Telecommunications Working Party.
II. OUTCOME OF PROCEEDINGS

The Working Party has prepared a draft Directive, contained in 6599/96 ECO 110 CODEC 225, which it submits to the Permanent Representatives Committee with a view to enabling the Telecommunications Council to arrive at a common position of principle on this matter at its meeting on 29 May.

However, at this stage of the proceedings the draft still raises a number of questions which are outlined below.

It should also be noted that most delegations have maintained general linguistic scrutiny reservations on the draft (which was compiled on the basis of texts available only in English) and that two delegations (DK and E) continue to harbour doubts as to the need for this Directive.

1. Main questions still unresolved

   (a) Extension of the Directive to subscribers who are legal persons (Article 1 and recital 11)

   Article 1(2) of the draft Directive states that the provisions of the Directive also cover protection of the legitimate interests of subscribers who are legal persons.

   The F/NL and UK delegations entered reservations on such an extension, particularly as they failed to see how the concept of personal data could be reconciled with that of legal persons.
Other delegations (notably A and D) and the Cion urged that the present text be retained, the Cion stressing in particular that in practice it was very difficult to distinguish between private persons and legal persons when it came to subscribers.

(b) Services provided via analogue networks (Article 3)

This Article specifies that the services covered by the Directive are publicly available telecommunications services provided via public telecommunications networks and in particular the ISDN Digital Network and public digital mobile networks.

The present text thus also covers analogue networks even though they do not guarantee a high level of security for users on the same conditions, notably as regards cost, as digital networks.

To satisfy the concern expressed by several delegations (DK/E/NL/P and S) in this connection, Article 4 states that the provider of a service must take measures to ensure a level of security appropriate to the risk presented having regard to the latest technical options available and the cost of their implementation.

The E delegation would have preferred a different wording, referring first to digital networks and then specifying that analogue networks were covered only where this was technically feasible or did not involve a disproportionate effort; it maintained a scrutiny reservation on Article 3 at this stage.
(c) **Particular risk of breach of security of the network and possible remedies (Article 4(2))**

Article 4(2) states that in the event of a particular risk of a breach of the security of the network (e.g. in the field of mobile telephony), the subscriber must be informed of the risk and any possible remedies (including the costs involved).

The **L** delegation and the **Cion** representative maintained reservations on this provision, considering that the subscriber should not only be informed of such risk but should also be offered encryption facilities by the service provider.

The **L** delegation was however amenable to the Presidency's suggestion that a recital be introduced referring to encoding as an appropriate means of obviating the risk of security breaches.

(d) **Confidentiality of communications (Article 5)**

This Article concerning surveillance of communications, which was simplified by the Working Party, simply calls on Member States to ensure confidentiality, in particular by prohibiting listening in, tapping, storing or any other kinds of interception or surveillance of communications by persons other than users without the latters' consent. At the same time Article 15(1) allows Member States to derogate from this Article in order to safeguard national security, defence and public safety and to combat crime.

The **DK/F and NL** delegations maintained reservations on this Article, querying in particular whether Article 100a was an adequate basis for a provision of this kind.

It should also be noted that the text of Article 15(1), which was proposed by the Presidency during the most recent stage of the Working Party's proceedings on the Directive, has not yet been approved by all the delegations. (Several delegations felt that a provision of this kind might create some confusion in relation to Article 1(3) on the exclusion of the third pillar from the scope of the Directive).
(e) **Entitlement to be omitted from the directory free of charge (Article 11)**

The current wording of Article 11 states that the subscriber shall be entitled, free of charge, to be omitted from the directory at his or her request.

The E delegation was vigorously opposed to this entitlement being free, arguing that such a provision could not only undermine the credibility of the directory but could also adversely affect operators' turnover. It therefore requested that this remain a matter for the Member States as was already the case in Directive 95/62/EC on voice telephony ONP (Article 16).

(f) **Adaptation of technical provisions contained in certain articles (Article 14)**

There was a broad consensus in the Working Party that it should be possible to adapt, in keeping with technological developments, the technical provisions contained in certain articles, and only that type of provision, by a simplified procedure (see (g) below in this connection).

Most delegations were agreed that the articles to be covered by this provision should be Article 4 (security), Article 6 (traffic and billing data), Article 8 (calling and connected line identification) and Article 10 (call forwarding).

The Commission representative, however, wanted this list to include Article 7 (itemized billing) and Article 12 (unsolicited calls); the L delegation supported him in the case of Article 12.
The Presidency has in the meantime drafted a new version of Article 14 and a new recital to go with it which reflect the Working Party's position on this matter; they were incorporated in the draft Directive submitted to the Permanent Representatives Committee.

(g) Committee procedure (Article 15(4))

The current text states that the Commission will be assisted by the Committee established by Article 31 of the general Directive on personal data protection (procedure II(b)).

The E/DK/NL/P/UK/S delegations wanted procedure III(b) to apply in the context of this Directive.

The Commission representative said that he was bound to keep to the text proposed by the Commission (advisory committee).

2. Other reservations

Apart from the matters outlined above, a number of specific points in the draft are still subject to reservations (or requests for textual amendments) by delegations.

These points, indicated in footnotes in 6599/96, are as follows:

- recital 10 (addition requested by UK)
- recital 11 (reservation by F)
- recital 12 (addition suggested by UK)
- recital 21 (reservation by UK)
- recital 23 (addition wanted by UK)
– Article 5 (addition wanted by \textit{F and UK})
– Article 6(2) (reservation by \textit{F}, which wanted an unrestricted list)
– Article 6(5) (reservation by \textit{P})
– Article 8(2) (reservations by \textit{F/UK/FIN/S}, scrutiny reservations by \textit{NL and IRL})
– Article 8(2)(b) (reservation by \textit{F}, scrutiny reservation by \textit{UK})
– Article 10 (addition requested by \textit{D})
– Article 11 (textual amendments wanted by \textit{D/NL and UK})
– Article 15(3) (reservation by \textit{F}).

In addition, Article 12 (unsolicited calls), which does not pose any problems, will need to be redrafted to reflect the Working Party's conclusions.
EUROPEAN UNION
THE COUNCIL

Brussels, 31 May 1996

7784/96

LIMITE
ECO 153
CODEC 348

OUTCOME OF PROCEEDINGS

from: Working Party on Economic Questions (Data Protection)
dated: 29 May 1996

No. prev. doc.: 6599/96 ECO 110 CODEC 225
No. Cion prop.: 7966/94 ECO 156

Subject: Modified 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks

In accordance with the mandate of COREPER the Working Party reexamined the abovementioned directive on 29 May.

The text of this Directive as it stands at the end of this meeting is contained in the Annex to the present document; the remaining reservations are set out in the Report of the Working Party to COREPER (doc. 7785/96 ECO 154 CODEC 349).
ANNEX

DRAFT DIRECTIVE
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR, IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND IN THE PUBLIC DIGITAL MOBILE NETWORKS

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission,

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

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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) Whereas currently in the European Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;
(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;

(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonised in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8A of the Treaty; whereas the harmonisation pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks in more than one Member State will not be hindered;

(8) Whereas these new services include interactive television and video on demand;

(9) Whereas in the telecommunications sector, 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 the individual, Directive
95/46/EC shall apply; whereas Directive 95/46/EC shall apply to non publicly available telecommunication services;

(10) Whereas this Directive, in conformity with article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law;

(11) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of the said Directive 95/46/EC to the protection of the legitimate interests of legal persons;

(11bis) Whereas service providers must take appropriate measures to safeguard the security of their services, and inform subscribers about any special risks of a breach of the security of the network and about any possible remedies which may include encryption facilities;

(12) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications;

(13) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern their right to respect for correspondence; whereas 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; whereas any further processing which the provider of the publicly available telecommunication service may want to perform for the marketing of its own telecommunications 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 telecommunications service about the types of further processing he intends to perform;

(14) Whereas the introduction of itemised bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider, at the same time it may
jeopardise the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemised bills;

(15) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in exceptional cases; whereas certain subscribers, in particular helplines and similar organisations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right 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; whereas the providers of publicly available telecommunications services must inform their subscribers about the existence of calling and connected line identification in the network and about all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;

(16) Whereas directories are widely distributed and publicly available; whereas the right to privacy requires that the subscriber himself is able to determine to which extent his personal data are published in a directory;

(17) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas in such cases it must be possible for the subscriber to stop the forwarded calls being passed on to his terminal by simple request to the provider of the publicly available telecommunications service;
(18) Whereas safeguards must be provided for the users against intrusion into their privacy by means of unsolicited calls and telefaxes;

(19) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(20) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(21) Whereas Member States, industries concerned and the European Community will have to cooperate in developing and manufacturing the technologies necessary for the implementation of this Directive; this cooperation will have to respect in particular the competition rules of the Treaty;

(22) Whereas 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 telecommunications 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 State security;

(23) Whereas 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 in Article 29 of Directive 95/46/EC;

(24) Whereas given the technological developments in the telecommunications sector and the attendant evolution of the services on offer, it will be necessary to determine the technical modalities necessary for the application of certain provisions of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of
Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

HAVE ADOPTED THIS DIRECTIVE:

Article 1
(Object and scope)

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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 the activities which fall outside the scope of Community law, such as those provided for 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)

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) 'subscriber' means any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;

(b) 'user' means any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) 'public telecommunications network' means transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) 'telecommunications service' means services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio-and television broadcasting.
Article 3
(Services concerned)

This Directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services supported by public telecommunications digital networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

It also applies to the processing of personal data in connection with the provision of publicly available telecommunications services supported by public telecommunications analogue networks where technically possible and it does not involve disproportionate economic effort.

Article 4
(Security)

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications service must inform the subscribers
concerning such risk and any possible remedies, including the costs involved.

Article 5

(Confidentiality of the communications)

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit unauthorised listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned.

Article 6

(Traffic and billing data)

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.
3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection disputes.

Article 7
(Itemized billing)

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge, to prevent the presentation of the calling line identification of incoming calls.

2bis. 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 via a simple means, free of charge for reasonable use of this function, to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

3. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

4. The provisions set out in paragraphs 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2 and 3 shall also apply to incoming calls originating in third countries.
5. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2 and 3.

Article 9
(Exceptions)

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.
Article 10
(Automatic call forwarding)

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

Article 11
(Directories of subscribers)

Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference added revealing his or her sex.

Article 12
(Unsolicited calls)

1. Notwithstanding the provisions of Directive .../... on the protection of consumers in respect of contracts negotiated at a distance (distance selling), Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing are not allowed either
without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, as determined by national legislation.

2. The use of automatic call devices for transmitting pre-recorded voice, telefax or other messages for purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

3. Member States may limit the application of this article to subscribers who are natural persons.

Article 13
(Technical features and standardization)

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council Directive 83/189/EEC which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of
specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications.

[Article 14]

Article 15

(Extension of the scope of application of certain provisions of Directive 95/46/EC)

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and 8, para. 1 and 3, 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 telecommunications system, as referred to in Article 13 para. 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks
laid down in Article 30 of the above-mentioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.

**Article 16**

*Implementation of the Directive*

1. The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.

When Member States adopt these provisions, these shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By derogation to the last sentence of Article 6.3, consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.
3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.

Article 17

(Addressees)

This Directive is addressed to the Member States.
List of traffic and billing data

For the purpose referred to in Article 6.2 the following data may be processed:

Data containing the:

- number or identification of the subscriber station,

- the address of the subscriber and the type of station,

- total number of units to be charged for the accounting period,

- called subscriber number,

- type, start time and duration of the calls made and/or the data volume transmitted,

- other information concerning payments such as advance payment, payments for instalsments, disconnection and reminders.
REPORT

from: Working Party on Economic Questions (Data Protection)
on: 29 May 1996
to: Permanent Representatives Committee

No. prev. doc.: 7784/96 ECO 153 CODEC 348
No. Cion prop.: 7966/94 ECO 156

Subject: Amended proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the context of digital telecommunications networks (ISDN)

At its meeting on 29 May 1996, the Working Party re-examined the above Directive as instructed by Coreper on 3 May 1996 (see 7065/96 EXT 2 and ADD 1 thereto).

The outcome of this discussion is given below, while the amended text resulting from this meeting will be found in 7784/96 ECO 153 CODEC 348.

°

° °
I. MAIN QUESTIONS OUTSTANDING

1. Extension of the Directive to subscribers who are legal persons: Article 1(2)

The text revised by the Working Party retains the general principle of including legal persons within the scope of the Directive while allowing Member States the option of not applying Article 12 to such persons (see new paragraph 3 of that Article).

This solution, which was proposed by the Presidency in order to satisfy the three delegations (F/NL/UK) maintaining reservations on this question, prompted the following positions:

- a very large majority of delegations were in favour; (¹)

- NL/UK delegations reacted positively and undertook to examine the proposal in a constructive frame of mind;

- F was cautious as it thought that this clause should at least be extended to Article 6(3) (concerning data processing for the purpose of marketing telecommunications services) (²).

(¹) However, one of these delegations (P) wondered about the risk of distortions which might be caused by the Article 12 clause in view of its optional nature.

(²) It should be noted that the French suggestion that in Article 6(3) the present "opt-in" solution (prior consent of the subscriber) should be replaced by an "opt-out" solution (possibility for the subscriber of opposing processing) was supported by FIN/UK while the Chairman was prepared to consider this suggestion.
2. **Services provided through analogue networks: Article 3**

The new wording of this Article stipulates that services provided through analogue networks shall be covered only where technically possible or where this does not involve disproportionate economic effort.

This solution was adopted by the Presidency, which thought that it was the most likely way of achieving a consensus on this question.

However, the Cion representative entered the most trenchant reservations on this solution and said that he would prefer the alternative solution, which was also examined at the Working Party meeting and limits this clause to Articles 8, 9 and 10 on the basis of a Community procedure (solution which was also preferred by certain delegations, in particular A/S/UK, which feared distortions of competition). (3)

3. **Security of the network and encryption: Article 4(2)**

In order to take account of the concerns of both L (which would like operators to offer their subscribers practical solutions for safeguarding security) and the Cion representative (who wanted a reference to the possibility of encryption), the Chairman proposed inserting a new recital reading as follows:

---

(3) Under this alternative solution, the previous text would be supplemented as follows: "In cases where, due to the technical level of the network, it would be impossible or require a disproportionate investment to fulfil the requirements of Articles 8, 9 and 10 of this Directive, Member States may be granted a temporary derogation, where justified, under the committee procedure mentioned in Article 15(4)."
"(11a) Whereas service providers must take appropriate measures to safeguard the security of their services, and inform subscribers about any special risks of a breach of the security of the network and about any possible remedies which may include encryption facilities;"

The following reservations were, however, upheld on this solution:

– substantive reservation by L;

– request by NL that the words "which may include encryption facilities" in the final line should be deleted and the following added: "In the case of analogue mobile network, service providers are not obliged to offer encryption facilities";

– scrutiny reservations by A/D/F/S/UK.

4. Confidentiality of the communications: Article 5

With the exception of F/UK, which upheld a reservation of principle and a scrutiny reservation respectively, all delegations were able to accept or were favourably disposed towards the new wording of this Article. (4)

5. Absence of charges for exercising the right to be omitted from a telephone directory: Article 11

F upheld its opposition to such absence of charges.

(4) It should be noted however that A suggested supplementing this provision with the words "in accordance with Article 15(1)".
6. **Adaptation of certain provisions to technical progress: Articles 6(2), 15(4) and Annex**;

   **Committee procedure: Article 15(4)**

Since most of the delegations acknowledged that adaptation of the Directive to technical progress was only really a problem in the case of Article 6(2) concerning personal data relating to subscriber billing and interconnection payments, the following solution was envisaged by the Working Party:

(i) include in an Annex to the Directive an exhaustive list of the data which can be processed;

(ii) provide for the regulatory committee procedure referred to in Article 31 of the general Directive (type IIb procedure) for adapting this Annex rapidly and at a purely technical level to developments in telecommunications services.

However, this solution still prompted the following reservations:

– reservations by the D/L/A delegations, whose concerns were also shared by P, and who feared that such adaptation might alter the level of protection provided by this list, which they thought should not be done purely on the basis of a Committee procedure. In order to allay these concerns, the Presidency suggested making it clear in a recital that this procedure did not make it possible to go beyond purely technical adaptation;

– reservation by F on the general approach envisaged, as this delegation wanted a provision for this area that was more generally worded and subject to controls by
national authorities regarding data protection;

- scrutiny reservations by B/FIN.

II. OTHER RESERVATIONS

- Heading of the Directive: amendment suggested by EL:
  "...concerning the processing of personal data and the protection of privacy, the security of the network and the confidentiality of the communications in the telecommunications sector";
- recitals Nos 8 and 9: D reservation;
- recitals Nos 10, 12 and 23: additions requested by UK (see 6599/96);
- recital No 21: UK reservation;
- Article 1(3): A wanted to align this paragraph fully on the equivalent provision in the general Directive by adding after "apply to" in the first line the words "the processing of data in the case of";
- Article 4(1): UK reservation;
- Article 6(1): P wanted to replace "traffic data relating to subscribers and users" with "traffic data containing personal data";
- Article 6(5): reservations by P on the words "interconnection disputes" and by UK, which wanted to delete the final line "in view ....";
- Article 7: P wanted to make clear that free calls would not be shown on the itemized bill;
- Articles 8 and 10: P reservation; B reservation on "on a per-call basis" in Article 8(1);
- Article 8(2): A/D/E/FIN/P scrutiny reservations;
- Article 10: B reservation and addition requested by D (see 6599/96);
- Article 11: NL/UK reservations on the words "or to have his or her address omitted in part"; EL scrutiny reservation (reference to gender);
– Article 15(1): P reservation;
– Article 16(2): FIN proposed referring to paragraphs 2 and 3 of Article 6.

In addition, F communicated the following additional reservations (announced at Coreper on 3 May) to the Secretariat during the meeting:

– recitals: general reservation, in particular Nos 6, 8, 11 and 12;
– Article 4(1): reservation on the idea of "security of services";
– Article 6(1): supported P's request;
– Article 6(4): delete "and it ....";
– Article 7(2): delete or turn into a recital;
– Article 8(1): add "permanently" before "on a per-line basis";
– Article 8(2): delete;
– Article 13(3): reservation on the time for revision of the Directive on terminal equipment;
– Article 15: reservation linked to its position on "legal persons".
OUTCOME OF PROCEEDINGS

from: COREPER and Counsellors of the Permanent Representations
dated: 19 June 1996
to: "Telecommunications" Council

No. prev. doc.: 7785/96 ECO 154 CODEC 349
No. Cion prop.: 7966/94 ECO 156

Subject: Modified proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in the digital mobile networks

Delegations will find hereafter, in view of the Telecommunications Council of 27 June, the text of the abovementioned Directive resulting from the work undertaken on this dossier.

The outstanding issues, which are just mentioned in the footnote in the present document, are presented in a more detailed manner in the report of COREPER to the Council (doc. 8467/96 ECO 184 CODEC 418).
DRAFT DIRECTIVE
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR, IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND IN THE PUBLIC DIGITAL MOBILE NETWORKS

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission,

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

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data 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) Whereas currently in the European Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(1) F maintained a general scrutiny reserve on the present wording of the recitals. This delegation maintained at the same time a general linguistic reservation.
(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 has called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council has re-emphasized the importance of the protection of personal data and privacy in its resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community;

(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonised in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8A of the Treaty; whereas the harmonisation pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks in more than one Member State will not be hindered;
(8) Whereas these new services include interactive television and video on demand;

(9) Whereas in the telecommunications sector, 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 the individual, Directive 95/46/EC shall apply; whereas Directive 95/46/EC shall apply to non publicly available telecommunication services;

(10) Whereas this Directive, in conformity with article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(11) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of the said Directive 95/46/EC to the protection of the legitimate interests of legal persons; whereas this protection is ensured within the framework of the applicable community and national legislation;

(11bis) Whereas service providers must take appropriate measures to safeguard the security of their services, and inform subscribers about any special risks of a breach of the security of the network and about any possible remedies which may include encryption.

(1) Scrutiny reserve by UK on deletion of the words "in particular".
(2) Scrutiny reserve by UK on the wording of the fourth line and the last five words.
facilities;

(11) whereas security is appraised in the light of the provision of article 17 of directive 95/46;(1)

(12) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications by means of public telecommunications network and publicly available telecommunications service; whereas national legislation in some Member States only prohibits intentional unauthorised access to communications;

(13) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern their right to respect for correspondence; whereas 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; whereas any further processing which the provider of the publicly available telecommunication service may want to perform for the marketing of its own telecommunications 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 telecommunications service about the types of further processing he intends to perform;

(14) Whereas the introduction of itemised bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider, at the same time it may jeopardise the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemised bills;

(1) Waiting reserve by A.
(15) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in exceptional cases; whereas certain subscribers, in particular helplines and similar organisations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right 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; whereas the providers of publicly available telecommunications services must inform their subscribers about the existence of calling and connected line identification in the network and about all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;

(16) Whereas directories are widely distributed and publicly available; whereas the right to privacy requires that the subscriber himself is able to determine to which extent his personal data are published in a directory;

(17) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas in such cases it must be possible for the subscriber to stop the forwarded calls being passed on to his terminal by simple request to the provider of the publicly available telecommunications service;

(18) Whereas safeguards must be provided for the users against intrusion into their privacy by means of unsolicited calls and telefaxes;
(19) Whereas it is necessary to ensure that the introduction of technical features of telecommunication equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(20) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

[(21)]

(22) Whereas 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 telecommunication 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 State security;

(23) Whereas 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 in Article 29 of Directive 95/46/EC;

(24) Whereas given the technological developments in the telecommunication sector and the attendant evolution of the services on offer, it will be necessary to determine the technical modalities necessary for the application of certain provisions of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

HAVE ADOPTED THIS DIRECTIVE:
Article 1
(Object and scope)

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons. (1)

3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for 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)

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) 'subscriber' means any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;

(b) 'user' means any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(1) Waiting reservation by F.
(c) 'public telecommunications network' means transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) 'telecommunications service' means services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio-and television broadcasting.

Article 3
(Services concerned)\(^{(1)}\)\(^{(2)}\)

1. This Directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 of the Directive 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, 9 and 10 of the Directive, shall be notified to the Commission by the Member States.

\(^{(1)}\) It was agreed to insert the following Declaration in the minutes of the Council: "The Council and the Commission note that nothing in the present Directive prevents a Member State from applying its provisions to non-public telecommunications and non-publicly available telecommunications services and that Directive 94/45/EC applies in any case to the processing of personal data in the framework of such networks and services".

\(^{(2)}\) A maintained a linguistic reserve on the wording of this article and \(F\) linked its definitive position to the outcome of the discussions in Article 8.
Article 4  
(Security)

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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.(1)

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.(2)

Article 5  
(Confidentiality of the communications)

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned except when legally authorised.(3)

Article 6  
(Traffic and billing data)

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of

(1) Reservation by UK.
(2) Reservation by LUX.
(3) Scrutiny reserve by UK on this article.
2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.(2)

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.(3)

**Article 7**

*(Itemized billing)*

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative modalities for communications or payments are available to such users and subscribers.

---

(1) Study reserve by F and Port.

(2) Reserve by UK and FIN which favour an "OPT OUT" solution.

(3) UK requested to delete last line "in view...".
**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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls.

2bis. 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 via a simple means, free of charge, for reasonable use of this function, to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

3. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

---

(1) F maintained a scrutiny reserve on the provisions contained in this article.
(2) Scrutiny reserve by DK and D on the words "for reasonable use of this function".
(3) Reservation by UK on the words "free of charge".
(4) It was agreed to insert in the minutes of the Council the following statement: "The Council and the Commission note that the provision of Article 8.2bis does not prevent Member States from prohibiting government agencies, public utilities and emergency services to reject calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber."
4. The provisions set out in paragraphs 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2 and 3 shall also apply to incoming calls originating in third countries.

5. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2 and 3.

Article 9
(Exceptions)

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.
Article 10
(Automatic call forwarding)

Member states shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.\(^1\)

Article 11
(Directories of subscribers)

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference added revealing his or her sex, where this is applicable linguistically.\(^2\)

2. Member states may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.

---

\(^1\) Port maintained a scrutiny reserve on this article. D requested to add the following provisions: "The calling subscriber must be informed automatically during the establishment of the connection that the call is being forwarded to a third party".

\(^2\) It was agreed that the accuracy of the expression "is applicable linguistically" will be checked by the jurist-linguists group.

\(^3\) It was agreed to insert the following statement in the minutes of the Council: "The Council and the Commission note that paragraph 2 of Article 11 reflects the provision which was agreed on the same subject matter by the Council of Europe in its Recommendation N° R(95)4 of 7 February 1995".

D maintained a linguistic reserve on this provision.
Member States may limit the application of this article to subscribers who are natural persons.

**Article 12**

*(Unsolicited calls)*

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) 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 calls for purposes of direct marketing, by other means 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 calls, the choice between these options to be determined by national legislation.

3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.

**Article 13**

*(Technical features and standardization)*

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs (2) and (3) of this Article, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications 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 only be implemented by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Council

---

(1) The new wording of this article (in conformity with the distance selling directive) was favourably received by delegations without prejudice to a scrutiny reserve by D., IRL, F., A., S and FIN.
Directive 83/189/EEC which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications.\(^{(1)}\)

[Article 14]

Article 15

(Extension of the scope of application of certain provisions of Directive 95/46/EC)\(^{(2)}\)

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and 8, para. 1, 2, 2bis and 3, 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 telecommunications system, as referred to in Article 13 para. 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article

\(^{(1)}\) P asked the confirmation by the Commission that the adoption of a modified Directive on terminal equipment be imminent.

\(^{(2)}\) Scrutiny reserve by P on the wording of this article.
protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.(1)

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.(2)

Article 16
(Implementation of the Directive)

1. The Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.(3)

When Member States adopt these provisions, these shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By derogation to the last sentence of Article 6.3, consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this

(1) It was agreed to insert the following declaration in the minutes of the Council:
"The Council and the Commission consider that the Working Party mentioned in Article 15.3 of the Directive, could for the purposes of this Directive, usefully draw on the expertise of the National Regulatory Authorities for Telecommunications by inviting where appropriate, the representatives of the NRAs as experts to its meetings".

(2) On the initiative of the Presidency it was agreed to insert the following statement in the minutes of the Council:
"The Council and the Commission note that the technical specifications to be made to the Annex according to the procedure referred to in Article 15 paragraph 4 shall in no way change the substance of Article 6, for example by adding or deleting categories of data, and should be limited to particularizing the list of data on account of changes in technology".

However, D. Lux, Port and UK maintained a scrutiny reserve on paragraph 4 and this declaration. Cion maintained a reserve on comitology.

(3) Reservation by F on this date.
into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. The Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.

Article 17
(Addressees)

This Directive is addressed to the Member States.
List of data

For the purpose referred to in Article 6.2 the following data may be processed:

Data containing the:

- number or identification of the subscriber station,
- the address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, start time and duration of the calls made and/or the data volume transmitted,
- other information concerning payments such as advance payment, payments for instalments, disconnection and reminders.
CORRIGENDUM TO THE OUTCOME OF PROCEEDINGS

from: COREPER and Counsellors of the Permanent Representations
dated: 19 June 1996
to: "Telecommunications" Council

No. prev. doc.: 7785/96 ECO 154 CODEC 349
No. Cion prop.: 7966/94 ECO 156

Subject: Modified proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in the digital mobile networks

Page 4, recital (9), first line

Take out the words "in particular".
CORRIGENDUM TO THE OUTCOME OF PROCEEDINGS
from: COREPER and Counsellors of the Permanent Representations
dated: 19 June 1996
to: "Telecommunications" Council

No. prev. doc.: 7785/96 ECO 154 CODEC 349
No. Com prop.: 7966/94 ECO 156

Subject: Modified proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in the digital mobile networks

Page 4 and 5, recital (11bis)

Delete the words "which may include encryption".
REPORT

from: Permanent Representatives Committee

on : 19 June 1996

to : TELECOMMUNICATIONS COUNCIL

No. prev. doc.: 8360/96 ECO 179 CODEC 406
No. Cion prop.: 8460/90 ECO 158 COM(90) 314 final SYN 284-288

Subject: Amended proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and digital mobile networks

I. INTRODUCTION

The Commission submitted the original proposal on 27 July 1990 at the same time as the proposal for a general Directive on the protection of individuals in relation to the processing of personal data.

The purpose of the proposal was to implement the general principles of the protection of personal data and privacy in the context of the specific requirements for digital telecommunications networks so as to preclude a situation where diverging developments within the Community might compromise the common market in telecommunications services and equipment.

The amended proposal now submitted for the Council's examination dates from October 1992; it takes account of the Opinion of the European Parliament and was fundamentally reassessed in the light of the principle of subsidiarity.

Examination of this proposal by the Council did not really begin until the second half of 1995, following final adoption of the general Directive in October 1995.
II. **OUTCOME OF PROCEEDINGS WITHIN THE COUNCIL**

The proceedings resulted in the preparation of the draft Directive set out in 8360/96, which is submitted to the Council to enable it to establish a common position of principle on the issue at its meeting on 27 June 1996.

Although the latest round of discussions (within Coreper and in the Working Party of Counsellors from the Permanent Representations acting on instructions from Coreper) enabled most of the problems raised by the Directive to be resolved, a number of reservations are still being maintained at this stage on the text of the draft.

These reservations are briefly summarized below.

- 
- 
- 

A. **PRINCIPAL QUESTIONS**

It has not yet proved possible entirely to resolve two of the six principal questions which were discussed in depth.

(i) **Article 4(2): particular risk of a breach of the security of telecommunications services**

For the purposes of the Directive, the concept of security means the effective protection of personal data in particular as regards the circulation of, or access to such data without authorization. Article 4(2) provides that where a particular risk of a breach of security exists (e.g. in the context of mobile networks) the service provider must inform its subscribers that such a risk exists and of any possible remedies.
The **LUX** delegation still maintained a reservation on this provision on the grounds that, in terms of data security, it fell short of the level of protection required by the framework Directive and in particular Article 17 on the security of processing.

The counter-argument put forward against this position was that Article 4(1) was entirely in line with the corresponding provision in Article 17 of the general Directive and that the information requirement laid down in Article 4(2) was additional to the measures provided for in the first paragraph. The **LUX** delegation undertook to review its position and stated that it might wish to submit a proposal for a joint statement by the Council and the Commission to clarify the issue.

(ii)  **Adaptation of certain provisions to technical developments: Article 15(4) and the Annex**

A list of data which may be processed by service providers in order to bill their subscribers is given in an Annex to the Directive.

As the telecommunications services sector is evolving rapidly, the question arose as to how this list could be adapted by means of a rapid procedure.

However, this question elicited differences of opinion between certain delegations, which were apprehensive that such an adaptation might change the level of protection guaranteed by the list and therefore preferred an Article 100a procedure, and other delegations, which thought that the latter procedure was too cumbersome to allow technical progress to be taken into account in a satisfactory manner.

Discussion of this point resulted in a favourable attitude towards the following solution which the Presidency is submitting to the Council for confirmation,
without prejudice to the scrutiny reservations still upheld by a number of delegations
(D/LUX/ Port and UK). (1)

– a Regulatory Committee procedure as referred to in Article 31 of the general Directive
(I Ib) for technical adaptation of the list (Article 15(4));

– entry in the Council minutes of the following statement:

"The Council and the Commission note that the technical specifications to be included
in the Annex according to the procedure referred to in Article 15(4) may in no way
change the substance of Article 6, for example by adding or deleting categories of
data, and should be limited to particularizing the list of data on account of changes in
technology."

(iii) Other reservations outstanding on one or other of the principal questions

Although a solution has been reached on the question of extending the Directive to
subscribers who are legal persons, the F delegation, which had submitted amendments on
Articles 1 and 15 with a view to improving their legal form to take account of such
extension (which amendments were not adopted) is maintaining a scrutiny reservation on
these provisions.

The A delegation is also upholding a provisional linguistic reservation on the wording of
Article 3.

(1) There is also a Cion reservation on the Committee procedure.
B. Reservations outstanding on the other questions (i)

(i) Recitals

- the F delegation maintained a general reservation on the recitals;
- the UK delegation maintained a scrutiny reservation on the wording of recital 10;
- the A delegation maintained a scrutiny reservation on recital 11b.

(ii) Article 4(1) (Security)

The UK delegation at this stage still maintained a reservation on paragraph 1 on the grounds that the obligations incumbent upon service providers under this provision could in certain cases be too severe. However, it undertook to review its position.

(iii) Article 5 (Confidentiality of communications)

The UK delegation maintained a scrutiny reservation on the wording of the Article (it had problems with the term "legally" in the second sentence).

(iv) Article 6 (Traffic and billing data)

- the Port delegation, whose concern was shared by F, maintained a scrutiny reservation on the expression "traffic data relating to subscribers and users" at the beginning of paragraph 1;
- on paragraph 3, the UK and FIN delegations preferred an OPT OUT solution (possibility for a subscriber to oppose such processing) instead of an OPT IN solution (prior consent);
- the UK delegation wanted the possibility available to the competent authorities to be informed of billing data, as provided for in paragraph 5, not to be confined to the settlement of disputes.

(\^) It should be noted that F maintained a general linguistic reservation on the entire text of the Directive.
(v) **Article 8 (Presentation of calling and connected line identification)**

- the F delegation thought that a number of the provisions in this Article were excessive (in particular in paragraphs 2 and 2a);
- on paragraph 2, the DK and D delegations maintained scrutiny reservations on the expression "for reasonable use of this function";
- the UK delegation maintained a reservation on the requirement for the service in paragraph 2a to be free of charge.

(vi) **Article 10 (Automatic call forwarding)**

- the Port delegation maintained a scrutiny reservation on the wording of this Article;
- the D delegation wanted an additional provision added stipulating that the subscriber must be informed automatically when his call was being forwarded to a third party.

(vii) **Article 12 (Unsolicited calls)**

The D/IRL/F/A/S and FIN delegations maintained scrutiny reservations on the new wording of this Article, which was introduced at the final stage of the discussions. (The new wording is more compatible with the Directive on distance selling, to which this Article refers).

(viii) **Article 13 (Standardization)**

The F delegation wanted the Commission to confirm (possibly orally at the Council meeting) that the proposal for an amendment of the Directive on terminal equipment would be adopted very soon.

(ix) **Article 16 (Implementation of the Directive)**

Paragraph 1 requires Member States to comply with the Directive by 24 October 1998 at the latest. The F delegation maintained a reservation and wanted Member States to be given a period of three years to transpose the Directive into national law.
ADDENDUM TO REPORT

from: Permanent Representatives Committee

on: 19 June 1996

to: TELECOMMUNICATIONS COUNCIL

No. prev. doc.: 8360/96 ECO 179 CODEC 406
No. Cion prop.: 8460/90 ECO 158 COM(90) 314 final SYN 284-288

Subject: Amended proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and digital mobile networks

Delegations will find below the text of a statement sent to the Secretariat by the Île-de-France delegation, which proposes that it be entered in the Council minutes to clarify the provisions of Article 4.

"Statement by the Commission and the Council
(Minutes of the Council meeting on 27 June 1996)
Re Article 4"

The Council and the Commission consider that Article 4(1) establishes a level of security for processing which is consistent with that stipulated in Article 17 of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Furthermore, the Council and the Commission consider that where, despite the security measures taken, there continues to be a particular risk of a breach of the security of the network, the provider of a telecommunications service, where applicable in conjunction with the provider of the public telecommunications network, has the additional obligation of informing individuals as to the existence of such a risk and any possible remedies.

Entry of this statement would enable the L delegation to withdraw its reservation on Article 4(2).
COMMON POSITION (EC) No /96
ADOPTED BY THE COUNCIL ON .........................
WITH A VIEW TO ADOPTING
DIRECTIVE 96/ /EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND
THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR,
IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN)
AND IN THE PUBLIC DIGITAL MOBILE NETWORKS
DIRECTIVE 96/  /EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of

calling the processing of personal data
and the protection of privacy in the telecommunications sector,
in particular in the integrated services digital network (ISDN)
and in the public digital mobile networks

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the Opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) OJ No C 200, 22.7.1994, p. 4.
(2) OJ No C 
(3) Opinion of the European Parliament of ...... (OJ No C ...) (not yet published in the Official Journal),
Council Common Position of ... (OJ No C ...) (not yet published in the Official Journal) and
Decision of the European Parliament of ... (OJ No C ...) (not yet published in the Official Journal).
Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1) 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;

Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (5), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (6);

---

(1) OJ No L281, 23.11.1995, p. 31.
(5) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(6) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8a of the Treaty; whereas the harmonization pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(8) Whereas these new services include interactive television and video on demand;

(9) Whereas, in the telecommunications sector, 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, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunication services;
(10) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(11) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case 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; whereas this protection is ensured within the framework of the applicable Community and national legislation;

(12) Whereas 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 must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;
(13) Whereas service providers must 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; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;

(14) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications by means of public telecommunications network and publicly available telecommunications service; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(15) Whereas the data relating to subscribers processed to establish calls 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; whereas 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; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications 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 telecommunications services about the types of further processing he intends to perform;
(16) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardize the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;

(17) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas 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; whereas the providers of publicly available telecommunications services must 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 and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;
(18) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, 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 telecommunications service;

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(21) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonized in order to be compatible with the implementation of the internal market;

(22) Whereas 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 telecommunications 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 State security;
(23) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(24) Whereas 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;

(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

(26) Whereas, 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
Object and scope

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications 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 the activities which fall outside the scope of Community law, such as those provided for 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

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) "subscriber" shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;
(b) "user" shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) "public telecommunications network" shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) "telecommunications service" shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

**Article 3**

**Services concerned**

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 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, 9 and 10 shall be notified to the Commission by the Member States.
Article 4
Security

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5
Confidentiality of the communications

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.

Article 6
Traffic and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider’s own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

**Article 7**

**Itemized billing**

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge for reasonable use of this function, to prevent 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 via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in 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 telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.
Article 9
Exceptions

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10
Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber’s terminal.
Article 11
Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.

2. Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.

3. Member States may limit the application of this Article to subscribers who are natural persons.

Article 12
Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) 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 calls 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 calls, the choice between these options to be determined by national legislation.
3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.

**Article 13**

Technical features and standardization

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 telecommunications 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, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications (8).

---


Article 14
Extension of the scope of application of certain provisions of
Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), 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 unauthorized use of the telecommunications 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.

Article 15
Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.
When Member States adopt these provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By derogation from the last sentence of Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. 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.

**Article 16**

Addressees

This Directive is addressed to the Member States.

Done at

For the European Parliament

The President

For the Council

The President
List of data

For the purpose referred to in Article 6(2) the following data may be processed:

Data containing the:

- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, start time and duration of the calls made and/or the data volume transmitted,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.
COMMON POSITION (EC) No 8937/96
ADOPTED BY THE COUNCIL ON ...
WITH A VIEW TO ADOPTING
A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY
IN THE TELECOMMUNICATIONS SECTOR,
IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN)
AND IN THE DIGITAL MOBILE NETWORKS

DRAFT STATEMENT OF THE COUNCIL'S REASONS
I. **INTRODUCTION**

On 27 July 1990 the Commission submitted a proposal for a Directive, based on Article 100a EC, concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks.


After re-examining its proposal in the light of those Opinions, the Commission submitted an amended proposal to the European Parliament and the Council.

The Council adopted its common position in accordance with Article 189b of the Treaty on ....

II. **AIM OF THE PROPOSAL**

The proposal sets out to apply for the specific purposes of telecommunications networks the general data protection principles laid down by Directive 95/49/EC of the European Parliament and of the Council of 24 October 1995. It is accordingly designed, in a constantly changing field, to prevent Member States' legislation from developing along different lines in ways that might jeopardize the single market in telecommunications services and terminal equipment, while ensuring a high level of protection of the rights of individuals, in particular their right to privacy.
III. ASSESSMENT OF THE COMMON POSITION

1. **General comments**

The common position adopted by the Council provides confirmation of the approach followed by the Commission in its amended proposal and of the Commission's objectives, even though the Council has been prompted to make some changes to the detailed provisions of that proposal.

In making such amendments, the Council was generally concerned to:

– align the provisions of this Directive on those of the general Directive (particularly as regards the scope, Articles 1 and 14);

– ensure that they are consistent with the Community rules already adopted or in preparation in the telecommunications sector (e.g. the definitions in Article 2);

– clarify the scope of some provisions or make them more flexible.

2. **Specific comments**

(i) With regard to the European Parliament's amendments, the Council took the following line:

– Amendment No 96, first part (private networks and services)

Article 3 of the common position stipulates that the Directive applies to publicly available telecommunications services provided in public telecommunications networks. However, that Article is to be construed as allowing a Member State to apply its provisions to non-public or non-publicly available networks and services, with the proviso that Directive 95/46/EC in any case applies to the processing of personal data in the context of such networks and services.
– Amendment No 97 (development of technologies)

The Council went along with the Commission, which did not include in its amended proposal the new recital 21a proposed by the European Parliament.

– Amendments Nos 96, second part (value-added services), 98 (special or exclusive rights), 107 and 108 (service providers other than telecommunications organizations)

These amendments could not be accepted as they were no longer consistent with the legal situation brought about by the new Community rules governing the telecommunications sector.

– Amendment No 99

The definition of a telecommunications service given in this amendment has been included in Article 2(d).

– Amendment No 100 (directories of subscribers)

The content of this amendment has mainly been included in Article 11 of the common position.

However, under that provision, the principle that the right to be omitted from the directory is applicable free of charge may be departed from, subject to certain conditions. Article 11(2) stipulates that Member States may allow operators to require a payment from subscribers for exercising that right, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of the right.

It should be noted that this paragraph is to be construed as reflecting the provision agreed on the same subject matter by the Council of Europe in its Recommendation No R(95)4 of 7 February 1995.

– Amendment No 101 (electronic profiles of subscribers)

The Council took the same line as the Commission in not including Article 4 of the original proposal, to which the amendment related. However, it believes that the protection sought by the European Parliament is in any event ensured, in general terms by Directive 95/46/EC and in the specific case of traffic and billing data by Article 6 of the common position, in particular paragraph 3.

– Amendment No 102 (protection of the contents of information transmitted)

The Council took the same line as the Commission in not including
Article 5 of the original proposal, to which the amendment related. (see the following point for traffic and billing data).

– Amendments Nos 103 and 104 (traffic and billing data)

The points about which the European Parliament was concerned have been accommodated in the various paragraphs of Article 6 of the common position.

The provision put forward by the Commission in its amended proposal with regard to traffic data is included in Article 6(1). (The Council has also followed the Commission in not including the provision corresponding to Article 10(1) of the original proposal – the subject of amendment No 103 – which is already taken into account in the general Directive).

The provisions on billing data (Article 9 of the original proposal, Article 5 of the amended proposal) have been included in Article 6(2), with an exhaustive list of data which may be processed for the purpose of subscriber billing now being given in an Annex to the Directive, in the interests of ensuring a high level of protection.

Under Article 14(4) of the common position, that list, which is the same as the one proposed by the Commission and endorsed by the European Parliament, may only be technically specified by the Committee established by Article 31 of Directive 95/46/EC (see Article 14(4)). This provision is to be construed as in no way allowing the substance of the Annex and of Article 6 to be changed, e.g. by adding or deleting categories of data, and as merely permitting the list of data to be particularized on account of changes in technology. Substantial amendments calling into question data protection may therefore be introduced only under the procedure laid down in Article 100a of the Treaty.

All data other than those listed in that Annex to the common position, moreover, should be regarded as having to be processed in accordance with the principles in Directive 95/46/EC, especially Article 16 of it.

Article 6(4) of the common position contains provisions on restriction of access to traffic and billing data that accommodate the concern expressed by the European Parliament in amendment No 103.
– Amendment No 105 (automatic call forwarding)

This amendment is to a large extent taken into account in Article 10 of the common position, which enjoins Member States to ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

– Amendment No 106 (teleshopping service)

The provisions contained in Article 16 of the original proposal have been omitted from the common position, as the European Parliament wished.

(ii) The main other changes made in the common position are as follows:

– Article 3: the Directive applies to services provided via digital and analogue networks. However, the provisions of Articles 8, 9 (presentation of line identification) and 10 (automatic call forwarding) are applicable to subscriber lines connected to analogue exchanges only where technically possible and if this does not require a disproportionate economic effort (paragraphs 2 and 3).

– Article 4 (security)

This Article corresponds to Article 8 of the original proposal.

The Article is to be understood as follows:

= the provisions of paragraph 1 are designed to establish a level of processing security consistent with that advocated by Article 17 of Directive 95/46/EC;

= as regards the provisions of paragraph 2, where, in spite of the security measures taken, there is still a particular risk of a breach of the security of the network, the provider of a telecommunications service, where appropriate together with the provider of the public telecommunications network, is in addition required to inform individuals of that risk and of possible remedies.

– Article 5 (confidentiality of communications)

The provisions on confidentiality of communications (Article 12 of the Commission proposal) have been redrafted more concisely and placed at the start of the enacting terms, after the provisions on security, in order to
highlight the importance to be attached to that principle.

- **Article 7 (itemized billing)**

The Council has opted for a wording which reconciles the right of subscribers to be able to check the correctness of their bills with the right to the protection of privacy; recital 16 also stipulates that Member States may, in order to protect users' privacy more effectively, opt to require the deletion of a number of digits from the called number mentioned in itemized bills.

- **Article 8 (presentation of calling and connected line identification)**

The provisions in the amended Commission proposal with regard to calling line identification have been redrafted so as not to be dependent upon any particular technology or terminal equipment and provisions on the connected line identification service have also been added.

With specific reference to the possibility, under paragraph 3, of rejecting a call from a user who has eliminated the presentation of identification of his line, it should be noted that this provision does not prevent Member States from prohibiting government agencies, public utilities and emergency services from rejecting calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

- **Article 12 (unsolicited calls)**

The provisions of this Article have been redrafted so as to tally with Article 10 of the common position for the Directive on distance selling.

- **Article 15 of the amended proposal (technical application and modification)**

This Article has been deleted and technical adaptation is now confined to the Annex, under the procedure laid down in Article 31 of Directive 95/46/EC (see the comments above on Parliament's amendments Nos 103 and 104).

- **Article 14(3) (Working Party on the Protection of Individuals)**

The Council, supported by the Commission, considers that the Working Party, set up under Article 29 of Directive 95/46/EC, which also has a role to play in the implementation of this Directive, could for the purposes of the Directive usefully draw on the expertise of the national regulatory authorities for telecommunications by where appropriate inviting
representatives of those authorities to its meetings as experts.

- **Article 15** (implementation of the Directive)

For transposition of the Directive into national law in the Member States, the Council has opted for the same time limit as for the general Directive, with a deadline of 24 October 1998.
CORRIGENDUM

Subject: Common position adopted by the Council with a view to adopting Directive 96/ /EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks

Page 5, recital (14), third line

"network" and "service" shall be replaced by "networks" and "services".
DIRECTIVE 96/.../EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of

concerning the processing of personal data
and the protection of privacy in the telecommunications sector,
in particular in the integrated services digital network (ISDN)
and in the public digital mobile networks

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the Opinion of the Economic and Social Committee (2),

Having regard to the Opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

---

(1) OJ No C 200, 22.7.1994, p. 4.
(2) OJ No C (not yet published in the Official Journal),
(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (\(^1\)) 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) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(3) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(4) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (\(^5\)), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (\(^6\));

\(^{1}\) OJ No L281, 23.11.1995, p. 31.
\(^{6}\) OJ No C 196, 1. 8.1989, p. 4.
Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8a of the Treaty; whereas the harmonization pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

Whereas these new services include interactive television and video on demand;

Whereas, in the telecommunications sector, 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, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunication services;
(10) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(11) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case 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; whereas this protection is ensured within the framework of the applicable Community and national legislation;

(12) Whereas 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 must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;
(13) Whereas service providers must 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; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;

(14) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(15) Whereas the data relating to subscribers processed to establish calls 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; whereas 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; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications 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 telecommunications services about the types of further processing he intends to perform;
(16) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardize the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;

(17) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas 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; whereas the providers of publicly available telecommunications services must 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 and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;
(18) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, 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 telecommunications service;

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(21) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonized in order to be compatible with the implementation of the internal market;

(22) Whereas 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 telecommunications 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 State security;
(23) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(24) Whereas 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;

(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

(26) Whereas, 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
Object and scope

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications 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 the activities which fall outside the scope of Community law, such as those provided for 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

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) "subscriber" shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;
(b) "user" shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) "public telecommunications network" shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) "telecommunications service" shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

**Article 3**

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 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, 9 and 10 shall be notified to the Commission by the Member States.
Article 4

Security

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5

Confidentiality of the communications

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.

Article 6

Traffic and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider’s own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

Article 7
Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge for reasonable use of this function, to prevent 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 via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in 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 telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.
Article 9
Exceptions

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10
Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber’s terminal.
Article 11
Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.

2. Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.

3. Member States may limit the application of this Article to subscribers who are natural persons.

Article 12
Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) 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 calls 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 calls, the choice between these options to be determined by national legislation.
3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.

**Article 13**

Technical features and standardization

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 telecommunications 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, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications (8).

---


Article 14

Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), 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 unauthorized use of the telecommunications 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.

Article 15

Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive by 24 October 1998 at the latest.
When Member States adopt these provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By derogation from the last sentence of Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. 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.

**Article 16**

Addressees

This Directive is addressed to the Member States.

Done at

For the European Parliament

The President

For the Council

The President
List of data

For the purpose referred to in Article 6(2) the following data may be processed:

Data containing the:

– number or identification of the subscriber station,

– address of the subscriber and the type of station,

– total number of units to be charged for the accounting period,

– called subscriber number,

– type, start time and duration of the calls made and/or the data volume transmitted,

– other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.
COMMON POSITION (EC) No 8937/96
ADOPTED BY THE COUNCIL ON 12 SEPTEMBER 1996
WITH A VIEW TO ADOPTING
A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY
IN THE TELECOMMUNICATIONS SECTOR,
IN PARTICULAR IN THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN)
AND IN THE DIGITAL MOBILE NETWORKS

STATEMENT OF THE COUNCIL'S REASONS
I. **INTRODUCTION**

On 27 July 1990 the Commission submitted a proposal for a Directive, based on Article 100a EC, concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks.


After re-examining its proposal in the light of those Opinions, the Commission submitted an amended proposal to the European Parliament and the Council.

The Council adopted its common position in accordance with Article 189b of the Treaty on 12 September 1996.

II. **AIM OF THE PROPOSAL**

The proposal sets out to apply for the specific purposes of telecommunications networks the general data protection principles laid down by Directive 95/49/EC of the European Parliament and of the Council of 24 October 1995. It is accordingly designed, in a constantly changing field, to prevent Member States' legislation from developing along different lines in ways that might jeopardize the single market in telecommunications services and terminal equipment, while ensuring a high level of protection of the rights of individuals, in particular their right to privacy.
III. **ASSESSMENT OF THE COMMON POSITION**

1. **General comments**

The common position adopted by the Council provides confirmation of the approach followed by the Commission in its amended proposal and of the Commission's objectives, even though the Council has been prompted to make some changes to the detailed provisions of that proposal.

In making such amendments, the Council was generally concerned to:

- align the provisions of this Directive on those of the general Directive (particularly as regards the scope, Articles 1 and 14);

- ensure that they are consistent with the Community rules already adopted or in preparation in the telecommunications sector (e.g. the definitions in Article 2);

- clarify the scope of some provisions or make them more flexible.

2. **Specific comments**

(i) With regard to the European Parliament's amendments, the Council took the following line:

- Amendment No 96, first part (private networks and services)

  Article 3 of the common position stipulates that the Directive applies to publicly available telecommunications services provided in public telecommunications networks. However, that Article is to be construed as allowing a Member State to apply its provisions to non-public or non-publicly available networks and services, with the proviso that Directive 95/46/EC in any case applies to the processing of personal data in the context of such networks and services.
Amendment No 97 (development of technologies)

The Council went along with the Commission, which did not include in its amended proposal the new recital 21a proposed by the European Parliament.

Amendments Nos 96, second part (value-added services), 98 (special or exclusive rights), 107 and 108 (service providers other than telecommunications organizations)

These amendments could not be accepted as they were no longer consistent with the legal situation brought about by the new Community rules governing the telecommunications sector.

Amendment No 99

The definition of a telecommunications service given in this amendment has been included in Article 2(d).

Amendment No 100 (directories of subscribers)

The content of this amendment has mainly been included in Article 11 of the common position.

However, under that provision, the principle that the right to be omitted from the directory is applicable free of charge may be departed from, subject to certain conditions. Article 11(2) stipulates that Member States may allow operators to require a payment from subscribers for exercising that right, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of the right.

It should be noted that this paragraph is to be construed as reflecting the provision agreed on the same subject matter by the Council of Europe in its Recommendation No R(95)4 of 7 February 1995.

Amendment No 101 (electronic profiles of subscribers)

The Council took the same line as the Commission in not including Article 4 of the original proposal, to which the amendment related. However, it believes that the protection sought by the European Parliament is in any event ensured, in general terms by Directive 95/46/EC and in the specific case of traffic and billing data by Article 6 of the common position, in particular paragraph 3.

Amendment No 102 (protection of the contents of information transmitted)

The Council took the same line as the Commission in not including
Article 5 of the original proposal, to which the amendment related. (see the following point for traffic and billing data).

– Amendments Nos 103 and 104 (traffic and billing data)

The points about which the European Parliament was concerned have been accommodated in the various paragraphs of Article 6 of the common position.

The provision put forward by the Commission in its amended proposal with regard to traffic data is included in Article 6(1). (The Council has also followed the Commission in not including the provision corresponding to Article 10(1) of the original proposal – the subject of amendment No 103 – which is already taken into account in the general Directive).

The provisions on billing data (Article 9 of the original proposal, Article 5 of the amended proposal) have been included in Article 6(2), with an exhaustive list of data which may be processed for the purpose of subscriber billing now being given in an Annex to the Directive, in the interests of ensuring a high level of protection.

Under Article 14(4) of the common position, that list, which is the same as the one proposed by the Commission and endorsed by the European Parliament, may only be technically specified by the Committee established by Article 31 of Directive 95/46/EC (see Article 14(4)). This provision is to be construed as in no way allowing the substance of the Annex and of Article 6 to be changed, e.g. by adding or deleting categories of data, and as merely permitting the list of data to be particularized on account of changes in technology. Substantial amendments calling into question data protection may therefore be introduced only under the procedure laid down in Article 100a of the Treaty.

All data other than those listed in that Annex to the common position, moreover, should be regarded as having to be processed in accordance with the principles in Directive 95/46/EC, especially Article 16 of it.

Article 6(4) of the common position contains provisions on restriction of access to traffic and billing data that accommodate the concern expressed by the European Parliament in amendment No 103.
– Amendment No 105 (automatic call forwarding)

This amendment is to a large extent taken into account in Article 10 of the common position, which enjoins Member States to ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

– Amendment No 106 (teleshopping service)

The provisions contained in Article 16 of the original proposal have been omitted from the common position, as the European Parliament wished.

(ii) The main other changes made in the common position are as follows:

– Article 3: the Directive applies to services provided via digital and analogue networks. However, the provisions of Articles 8, 9 (presentation of line identification) and 10 (automatic call forwarding) are applicable to subscriber lines connected to analogue exchanges only where technically possible and if this does not require a disproportionate economic effort (paragraphs 2 and 3).

– Article 4 (security)

This Article corresponds to Article 8 of the original proposal.

The Article is to be understood as follows:

= the provisions of paragraph 1 are designed to establish a level of processing security consistent with that advocated by Article 17 of Directive 95/46/EC;

= as regards the provisions of paragraph 2, where, in spite of the security measures taken, there is still a particular risk of a breach of the security of the network, the provider of a telecommunications service, where appropriate together with the provider of the public telecommunications network, is in addition required to inform individuals of that risk and of possible remedies.

– Article 5 (confidentiality of communications)

The provisions on confidentiality of communications (Article 12 of the Commission proposal) have been redrafted more concisely and placed at the start of the enacting terms, after the provisions on security, in order to
highlight the importance to be attached to that principle.

– **Article 7 (itemized billing)**

The Council has opted for a wording which reconciles the right of subscribers to be able to check the correctness of their bills with the right to the protection of privacy; recital 16 also stipulates that Member States may, in order to protect users' privacy more effectively, opt to require the deletion of a number of digits from the called number mentioned in itemized bills.

– **Article 8 (presentation of calling and connected line identification)**

The provisions in the amended Commission proposal with regard to calling line identification have been redrafted so as not to be dependent upon any particular technology or terminal equipment and provisions on the connected line identification service have also been added.

With specific reference to the possibility, under paragraph 3, of rejecting a call from a user who has eliminated the presentation of identification of his line, it should be noted that this provision does not prevent Member States from prohibiting government agencies, public utilities and emergency services from rejecting calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

– **Article 12 (unsolicited calls)**

The provisions of this Article have been redrafted so as to tally with Article 10 of the common position for the Directive on distance selling.

– **Article 13 of the amended proposal (technical application and modification)**

This Article has been deleted and technical adaptation is now confined to the Annex, under the procedure laid down in Article 31 of Directive 95/46/EC (see the comments above on Parliament's amendments Nos 103 and 104).

– **Article 14(3) (Working Party on the Protection of Individuals)**

The Council, supported by the Commission, considers that the Working Party, set up under Article 29 of Directive 95/46/EC, which also has a role to play in the implementation of this Directive, could for the purposes of the Directive usefully draw on the expertise of the national regulatory authorities for telecommunications by where appropriate inviting
representatives of those authorities to its meetings as experts.

- **Article 15** (implementation of the Directive)

  For transposition of the Directive into national law in the Member States, the Council has opted for the same time limit as for the general Directive, with a deadline of 24 October 1998.
"I"/"A" ITEM NOTE

from : General Secretariat

dated : 31 July 1996

to : COREPER/COUNCIL

No. Cion prop.: 7966/94 ECO 156

Subject: Adoption of a common position on a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the integrated services digital network (ISDN) and digital mobile networks


2. Further to those Opinions, the Commission presented an amended proposal on 14 June 1994. At its meeting on 27 June 1996 the Telecommunications Council reached political agreement with a view to adopting a common position on this Directive.
3. In the meantime the recitals have been reexamined by the Working Party and the text of the common position has undergone legal/linguistic editing; COREPER could therefore recommend that the Council:

− in accordance with Article 189b EC and acting unanimously (1), adopt the common position on this Directive set out in 8937/96 ECO 198 CODEC 448, as an "A" item at a forthcoming meeting;

− at the same time adopt the draft statement of the Council's reasons in Addendum 1 to that document;

− approve the entry of the statements in the Annex in the minutes of its meeting.

______________

(1) The P delegation has stated, however, that it will abstain in the vote on the common position.
1. "The Portuguese delegation states that it is unable to endorse the common position on the Directive concerning the protection of personal data in the context of telecommunications networks, although it totally subscribes to its objectives.

The latest amendments to Article 3 do not properly reflect the technical problems arising in the field of analogue networks, since these problems exist at the level of both analogue exchanges, as has been recognized, and analogue subscriber access (even in the case of a digital exchange).

Accordingly, the Portuguese delegation will abstain at the time the decision on the Directive's adoption is taken."

2. re Article 3

"The Council and the Commission note that nothing in the present Directive prevents a Member State from applying its provisions to non-public telecommunications and non-publicly available telecommunications services and that Directive 95/46/EC applies in any case to the processing of personal data in the framework of such networks and services."

3. re Article 4

"The Council and the Commission consider that Article 4(1) establishes a level of security for processing which is consistent with that stipulated in Article 17 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Furthermore, the Council and the Commission consider that where, despite the security measures taken, there continues to be a particular risk of a breach of the security of the network, the provider of a telecommunications service, where applicable in conjunction

(*) These statements for the minutes are not confidential and may therefore be released to the public.
with the provider of the public telecommunications network, has the additional obligation of informing individuals as to the existence of such a risk and any possible remedies.”.

4. re Article 8(2a)

"The Council and the Commission note that the provision of Article 8(2a) does not prevent Member States from prohibiting government agencies, public utilities and emergency services to reject calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.".

5. re Article 11(2)

"The Council and the Commission note that paragraph 2 of Article 11 reflects the provision which was agreed on the same subject matter by the Council of Europe in its Recommendation No R(95)4 of 7 February 1995.”.

6. re Article 12(2)

"The Austrian delegation states that, in accordance with the margin of manoeuvre left to Member States by recital 71 of Directive 95/46/EC, Austria may apply its legislation on unsolicited calls for marketing purposes aimed at consumers residing in its territory insofar as such regulation does not concern the protection of individuals with regard to the processing of personal data.”.

7. re Article 15(3)

"The Council and the Commission consider that the Working Party mentioned in Article 15(3) of the Directive could, for the purposes of this Directive, usefully draw on the expertise of the National Regulatory Authorities for Telecommunications by inviting, where appropriate, the representatives of the NRAs as experts to its meetings.”.

8. re Article 15(4)

"The Council and the Commission note that the technical specifications to be included in the Annex according to the procedure referred to in Article 15(4) may in no way change the substance of Article 6, for example by adding or deleting categories of data, and should be limited to particularizing the list of data on account of changes in technology.”.
9. re Annex:

"The Council and the Commission state that any data other than those referred to in the Annex to this Directive are to be processed in accordance with the principles of Directive 95/46/EC, in particular Article 7(b) thereof.".
ADDENDUM TO "I"/"A" ITEM NOTE

from: General Secretariat
dated: 31 July 1996
to: COREPER/COUNCIL

No. Cion prop.: 7966/94 ECO 156

Subject: Adoption of a common position on a Directive of the European Parliament and of the Council concerning the protection of personal data and privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks

At the request of the Austrian delegation (COREPER, 6.9.96), the following statement is to be added to the Annex (1):

"1a Austria agrees to the existing text of the common position on the understanding that Article 5 is to be interpreted in the light of recital 14 and Article 14(1) as meaning that:

- prohibition can by its nature apply only to intentional infringements of confidentiality, and
- legal exceptions from such prohibition can be authorized only pursuant to Article 14(1)."

(1) Note also that statement 4 refers to Article 8(3) and not (2a).
COVER NOTE

Subject: Common position of the Council on the proposal for a Directive of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector

Delegations will find attached the Commission document – SEC(96) 1605 final.

from : D.F. WILLIAMSON, Secretary-General of the Commission

dated: 12 September 1996

to : Jürgen TRUMPF, Secretary-General of the Council of the European Union

Sir,


(Complimentary close).

(s.) D.F. WILLIAMSON
Secretary-General

Encl: SEC(96) 1605 final COD 288
EUROPEAN UNION
THE COUNCIL
Brussels, 30 October 1996 (06.11)
(OR. f)

11199/96

LIMITE
CODEC 632
ENER 147
FIN 519
ECO 298

"I/A" ITEM NOTE

from: General Secretariat

to: Permanent Representatives Committee/Council

Subject: Common positions of the Council on the:
- proposal for a Directive of the European Parliament and of the Council concerning common rules for the internal market in electricity (C4-0457/96 – 00/0384 (COD)), and
- 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in digital mobile networks (C4-0470/96 – 00/0288 (COD)),
- Additional scrutiny period

1. On 4 September 1996, the Council deposited at the European Parliament the common position of the Council with a view to adopting the
- Directive of the European Parliament and of the Council concerning common rules for the internal market in electricity (C4-0457/96 – 00/0384 (COD));

On 17 September 1996, the Council deposited at the European Parliament the common position of the Council with a view to adopting the
- Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in digital mobile networks (C4-0470/96 – 00/0288 (COD)).
2. By letters dated 23 October 1996 (11204/96 CODEC 633 PE-L 160 and 11205/96 CODEC 633 PE-L 161) and in accordance with Article 189b(7) of the Treaty, the European Parliament has requested the Council's agreement to an extension by one month of the three-month period it is allowed in paragraph 2 of the aforementioned Article in order to decide on the common positions of the Council, given the complex nature of the topic.

3. The Permanent Representatives Committee could recommend that the Council, among the "A" items on the agenda for one of its forthcoming meetings, approve the letter as annexed hereto.
Draft letter from the Council
to the European Parliament

Sir,

The Council has received your letter of 24 October 1996 in which, in accordance with Article 189b(7) of the Treaty, you request a one-month extension of the period allowed to the European Parliament in order to decide on the common positions of the Council concerning the:

- proposal for a Directive of the European Parliament and of the Council concerning common rules for the internal market in electricity (C4-0457/96 – 00/0384 (COD)), and

- 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 telecommunications sector, in particular in the Integrated Services Digital Network (ISDN) and in digital mobile networks (C4-0470/96 – 00/0288 (COD)).

The Council has decided to grant this request.

(Complimentary close).
Lors de sa séance du 19 septembre dernier, le Parlement européen a accusé réception de six positions communes du Conseil. Toutefois, pour l'une d'entre elles, le Président de la commission parlementaire compétente a attiré mon attention sur la nécessité de pouvoir disposer, compte tenu de la complexité du dossier, d'un mois supplémentaire pour que le Parlement puisse adopter sa recommandation pour la deuxième lecture.

Cette position commune est relative à une directive du Parlement européen et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques publiques (C4-0470/96 - 00/0288(COD)).

En conséquence, j'ai l'honneur, en application de l'article 189 B, para 7, du Traité instituant la Communauté européenne, de solliciter votre accord sur la prolongation du délai d'un mois.

(Formule de politesse).

(is.) Klaus HÄNSCH

11204/96

isd

F
DIRECTIVE 97/   /EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND
THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR

Joint text approved by the Conciliation Committee
provided for in Article 189b(4)
of the EC Treaty
DIRECTIVE 97/...EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of

certaining the processing of personal data
and the protection of privacy in the telecommunications sector

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the Opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure laid down in Article 189b of the Treaty (3), in the light of the joint text approved by the Conciliation Committee on 6 November 1997,

(1) OJ No C 200, 22.7.1994, p. 4.
(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1) 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) Whereas 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) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(1) OJ No L 281, 23.11.1995, p. 31.
(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (5), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (6);

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(8) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 7a of the Treaty; whereas the harmonization is limited to requirements that are necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(9) Whereas 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 the provisions of this Directive.

(10) Whereas these new services include interactive television and video on demand;

(11) Whereas, in the telecommunications sector, 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, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunication services;

(12) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;
Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case 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; whereas this protection is ensured within the framework of the applicable Community and national legislation;

Whereas 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 must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;

Whereas service providers must 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; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;
(16) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(17) Whereas the data relating to subscribers processed to establish calls 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; whereas 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; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications 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 telecommunications services about the types of further processing he intends to perform;

(18) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardize the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;
(19) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas 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; whereas the providers of publicly available telecommunications services must 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 and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;

(20) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, 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 telecommunications service;
(21) Whereas directories are widely distributed and publicly available; whereas the right to privacy of
natural persons and the legitimate interest of legal persons require that subscribers are able to
determine the extent to which their personal data are published in a directory; whereas Member States
may limit this possibility to subscribers who are natural persons;

(22) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of
unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who
are natural persons;

(23) Whereas it is necessary to ensure that the introduction of technical features of telecommunications
equipment for data protection purposes is harmonized in order to be compatible with the
implementation of the internal market;

(24) Whereas 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 telecommunications 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 State security;

(25) Whereas where the rights of the users and subscribers are not respected, national legislation must
provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by
private or public law, who fails to comply with the national measures taken under this Directive;
(26) Whereas 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;

(27) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology; whereas this procedure applies solely to specifications necessary to adapt the Annex to new technological developments, taking into consideration changes in market and consumer demand; whereas the Commission must duly inform the European Parliament of its intention to apply this procedure and whereas, otherwise, the procedure laid down in Article 100a of the Treaty shall apply;

(28) Whereas, 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
Object and scope

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications 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 the activities which fall outside the scope of Community law, such as those provided for 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

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) "subscriber" shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;
(b) "user" shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) "public telecommunications network" shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in all or in part, for the provision of publicly available telecommunications services;

(d) "telecommunications service" shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

**Article 3**

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 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, 9 and 10 shall be notified to the Commission by the Member States.

**Article 4**

**Security**

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications 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 via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with Article 14(1).
2. Paragraph 1 shall not affect any legally authorized recording of communications 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 and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider’s own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.
5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

Article 7
Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge for reasonable use of this function, to prevent 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 via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in 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 telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9
Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification:
(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10
Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber’s terminal.

Article 11
Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.
2. Notwithstanding paragraph 1, Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved does not act as a disincentive to the exercise of this right, and that, taking account of the quality requirements of the public directory in the light of the universal service, it is limited to the actual costs incurred by the operator for the necessary adaptation and updating of the list of subscribers not to be included in the public directory.

3. The rights conferred by paragraph 1 shall apply to subscribers who are natural persons. Member States shall also guarantee, 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 12**

Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) 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 calls 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 calls, the choice between these options to be determined by national legislation.

3. The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.
Article 13
Technical features and standardization

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 telecommunications 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, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications (8).


Article 14
Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), 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 unauthorized use of the telecommunications 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.
Article 15
Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998.

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with Article 5 of this Directive not later than 24 October 2000.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By way of derogation from Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. 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.
Article 16
Addressees

This Directive is addressed to the Member States.

Done at

For the European Parliament
The President

For the Council
The President
List of data

For the purpose referred to in Article 6(2) the following data may be processed:

Data containing the:

- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, starting time and duration of the calls made and/or the data volume transmitted,
- date of the call/service,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.
CORRIGENDUM

Subject: Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector

Page 17, Article 11(2), lines 5 and 6

For: "... the necessary adaptation and updating of the list ..."
Read: "... the adaptation and updating of the list ...".
CORRIGENDUM

Subject: Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector

Page 4, recital (11), last two words
For: "... telecommunication services;"
Read: "... telecommunications services;"

Page 11, Article 2(c), fourth line
For: "... in all or in part..."
Read: "... in whole or in part ..."

Page 12, Article 5(1), second line
For: "... by means of public telecommunications network ..."
Read: "... by means of a public telecommunications network ..."
DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
CONCERNING THE PROCESSING OF PERSONAL DATA AND
THE PROTECTION OF PRIVACY IN THE TELECOMMUNICATIONS SECTOR
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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (¹),

Having regard to the Opinion of the Economic and Social Committee (²),

Acting in accordance with the procedure laid down in Article 189b of the Treaty (³), in the light of the joint text approved by the Conciliation Committee on 6 November 1997,
(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data \(^{(1)}\) 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) Whereas 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) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

\(^{(1)}\) OJ L 281, 23.11.1995, p. 31.
(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (5), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (6);

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must 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 risk connected with automated storage and processing of data relating to subscribers and users;

(8) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 7a of the Treaty; whereas the harmonization is limited to requirements that are necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

Whereas 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 the provisions of this Directive.

Whereas these new services include interactive television and video on demand;

Whereas, in the telecommunications sector, 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, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunications services;

Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider 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; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;
(13) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case 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; whereas this protection is ensured within the framework of the applicable Community and national legislation;

(14) Whereas 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 must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;

(15) Whereas service providers must 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; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;
(16) Whereas measures must be taken to prevent the unauthorized access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(17) Whereas the data relating to subscribers processed to establish calls 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; whereas 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; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications 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 telecommunications services about the types of further processing he intends to perform;

(18) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardize the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;
(19) Whereas 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; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas 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; whereas the providers of publicly available telecommunications services must 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 and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas 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 telecommunications service;

(20) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, 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 telecommunications service;
(21) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(22) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(23) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonized in order to be compatible with the implementation of the internal market;

(24) Whereas 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 telecommunications 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 State security;

(25) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;
(26) Whereas 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;

(27) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology; whereas this procedure applies solely to specifications necessary to adapt the Annex to new technological developments, taking into consideration changes in market and consumer demand; whereas the Commission must duly inform the European Parliament of its intention to apply this procedure and whereas, otherwise, the procedure laid down in Article 100a of the Treaty shall apply;

(28) Whereas, 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
Object and scope

1. This Directive provides for the harmonization 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 telecommunications sector and to ensure the free movement of such data and of telecommunications 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 the activities which fall outside the scope of Community law, such as those provided for 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

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) "subscriber" shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;
(b) "user" shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) "public telecommunications network" shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in whole or in part, for the provision of publicly available telecommunications services;

(d) "telecommunications service" shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

Article 3

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 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, 9 and 10 shall be notified to the Commission by the Member States.

**Article 4**

**Security**

1. The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications 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 telecommunications 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 via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with Article 14(1).
2. Paragraph 1 shall not affect any legally authorized recording of communications 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 and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex 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 may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider’s own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.
5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

Article 7
Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative 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 via a simple means, free of charge, to eliminate 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 via a simple means, free of charge for reasonable use of this function, to prevent 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 via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in 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 telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

**Article 9**

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification:
(a) 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 telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10
Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber’s terminal.

Article 11
Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.
2. Notwithstanding paragraph 1, Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved does not act as a disincentive to the exercise of this right, and that, taking account of the quality requirements of the public directory in the light of the universal service, it is limited to the actual costs incurred by the operator for the adaptation and updating of the list of subscribers not to be included in the public directory.

3. The rights conferred by paragraph 1 shall apply to subscribers who are natural persons. Member States shall also guarantee, 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 12
Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) 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 calls 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 calls, the choice between these options to be determined by national legislation.

3. The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.
Article 13
Technical features and standardization

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 telecommunications 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, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications (8).

Article 14

Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), 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 unauthorized use of the telecommunications 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 according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.
Article 15
Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998.

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with Article 5 of this Directive not later than 24 October 2000.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By way of derogation from Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. 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.
Article 16
Addressees

This Directive is addressed to the Member States.

Done at

For the European Parliament
The President

For the Council
The President
List of data

For the purpose referred to in Article 6(2) the following data may be processed:

Data containing the:

– number or identification of the subscriber station,

– address of the subscriber and the type of station,

– total number of units to be charged for the accounting period,

– called subscriber number,

– type, starting time and duration of the calls made and/or the data volume transmitted,

– date of the call/service,

– other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.
INFORMATION NOTE

from: General Secretariat

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 telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (00/0288(COD))

– Outcome of the European Parliament's second reading (Strasbourg, 13-17 January 1997)

A. INTRODUCTION

On 18 December 1996 the Committee on Legal Affairs and Citizens' Rights unanimously approved the draft recommendation for the European Parliament's second reading, containing 10 amendments to the Council's common position.

The main aims of the amendments, as stated by Mr MEDINA ORTEGA when presenting his report to the full house, were to:

– clarify the title of the Directive (amendment 2);
– avoid application of the principle of subsidiarity to telecommunications harmonization because of the basically transnational nature of telecommunications networks and services (amendments 3 and 4);
– extend the protection of privacy to legal persons, albeit with exceptions (amendment 5);
– ensure that subscribers' right not to have their particulars entered in a directory is exercisable free of charge (amendment 9, to Article 11(2)).
The PPE and ELDR groups put two other amendments (11 and 12) to a vote in the full house.

All political groups supported the recommendation for the second reading and the amendments proposed by the rapporteur.

**B. VOTING**

The full house adopted 9 amendments by a very large majority (amendment 1 was not put to a vote as it only concerned the Spanish language version and amendments 11, from the ELDR group, and 12, from the PPE group, were rejected). The PSE also put to a vote (in a separate vote) the deletion of Article 11(3) of the common position (rejected by the full house) and the deletion of the second part of the 20th recital (approved by the full house). The PPE and PSE groups also put to a vote (in a separate vote) the deletion of Article 12(3) (approved by the full house).

The Commission's preliminary position on the amendments and other changes adopted, as stated by Mr KINNOCK, was that it:

- accepted amendments 2, 3, 4, 6, 7, 9 and 10 because they involved helpful further details and drafting improvements. In particular, the Commission agreed with the principle that the right to privacy should be exercisable free of charge, as proposed by the European Parliament through the deletion of Article 11(2) (amendment 9);

- rejected amendments 5 and 8 for the following reasons:

  (a) regarding amendment 5, Mr KINNOCK pointed out that Article 11(3) allowed Member States to limit the application of Article 11(1) and (2) to natural persons on the grounds that, in the case of legal persons, inclusion in a directory or otherwise was not a fundamental right but rather a legitimate interest, thus warranting different treatment. Moreover, the wording proposed by Parliament could be construed conversely as allowing Member States to require legal persons to be included in a directory;
(b) the Commission rejected amendment 8 (elimination of calling line identification) because this contained a drafting error. It could, however, support amendment 12 (rejected by the full house).

The deletion of Article 12(3) and of the second part of the 20th recital was opposed by Mr KINNOCK as there were good reasons to distinguish between the application of Article 12(1) and (2) (unsolicited calls) to natural persons and to legal persons. The option in paragraph 3 did not involve any lack of protection of the legitimate interests of legal persons; Member States could provide such protection by other means.

The Commission would, on the other hand, be able to agree to an addition to paragraph 3, reading as follows:

**Article 12(3)***

"3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons, to the extent that the legitimate interests of subscribers other than natural persons, and in particular those of small and medium-sized enterprises, remain sufficiently protected."
9. Personal data and protection of privacy

A4-0415/96

Decision on the common position adopted by the Council with a view to adopting a European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (C4-0470/96 - 0/0288(COD))

(Codecision procedure: second reading)

The European Parliament,

- having regard to the common position of the Council, C4-0470/96 - 00/0288(COD),
- having regard to its opinion at first reading (1) on the Commission proposal to Parliament and the Council, COM(90)0314 (2),
- having regard to the amended Commission proposal to Parliament and the Council, COM(94)0128 (3),
- having regard to Article 189b(2) of the EC Treaty,
- having regard to Rule 72 of its Rules of Procedure,
- having regard to the recommendation for second reading of the Committee on Legal Affairs and Citizens' Rights (A4-0415/96),

1. Amends the common position as follows;

2. Calls on the Commission to support Parliament's amendments in the opinion it is required to deliver pursuant to Article 189b(2)(d) of the EC Treaty;

3. Calls on the Council to approve all Parliament's amendments, amend its common position accordingly and definitively adopt the act;

4. Instructs its President to forward this decision to the Council and the Commission.

(2) OJ No C 277, 5.11.1990, p. 12.
(3) OJ No C 200, 22.7.1994, p. 4.
European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks. 

(Annex) 

DG F III 

Common position of the Council

Amendments by Parliament

(Amendment 2)

Title


(Amendment 3)

Recital 7

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8a of the Treaty; whereas the harmonization pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(7) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8a of the Treaty; whereas the application of the subsidiarity principle is not appropriate to harmonization in the telecommunications sector because of the essentially transnational nature of telecommunications networks and services and whereas, in any case, such harmonization will have to guarantee that the promotion and development of new telecommunications services and networks between Member States are not hindered;
(Amendment 4)
Recital 7a (new)

(7a) Whereas the Member States, providers and users concerned, together with the competent Community bodies, must cooperate in introducing and developing the relevant technologies needed to apply the guarantees provided for by the provisions of this Directive;

(Amendment 5)
Recital 19

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas, with regard to legal persons, exceptions to this general principle, when the legitimate interests of the subscriber run counter to other interests, such as the user's right to information, must be respected;

(Separate vote)
Recital 20

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes;
(Amendment 6)
Recital 25

(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology, and bearing in mind that this procedure cannot apply to substantial changes in these categories of data, which may be undertaken only in accordance with the procedure laid down in Article 100a of the Treaty;

(Amendment 7)
Article 5

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.

Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with Article 14(1).
(Amendment 8)
Article 9, introduction

Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification:

Member States shall lay down legal provisions governing the way in which the provider of a publicly available telecommunications service may eliminate presentation of the calling line identification:

(Amendment 9)
Article 11(2)

2. Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.

Deleted

(Separate vote)
Article 12(3)

3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.

Deleted

(Amendment 10)
ANNEX indent 5a (new)

- date of the call/service
OUTCOME OF PROCEEDINGS

of: "Telecommunications" Working Group

dated: 30 January 1997

No. prev. doc.: 5429/97 CODEC 36 ECO 14
No. Cion prop.: 7966/94 ECO 156

Subject: Proposal for a European Parliament and of the Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks

- Amendments in second reading of the European Parliament

1. At its session of 30 January the "Telecommunications" Working Group examined the ten amendments that the European Parliament proposed in second reading (see doc. (5429/97), taking into account the preliminary position of the Commission. The result of the examination showed that in all probability it would not be possible to accept all the amendments.

2. The position at this stage of the Group on the individual amendments is as follows:

   Amendment 2 (title)

   The title in the common position refers in particular to ISDN and digital mobile networks; the Parliament's amendment calls for deletion of this reference. The Commission supported this amendment as it more accurately reflects the content of the Directive. The Group however rejected this amendment, several delegations preferring to retain the emphasis on digital networks.
Amendment 3 on recital 7 (harmonisation and subsidiarity)

This amendment is intended to limit the extent of subsidiarity. The Commission supported the amendment whereas the Group could not accept it.

Amendment 4 on recital 7a (cooperation with a view to development of relevant technologies)

This amendment aims to ensure cooperation between all concerned parties in order to develop relevant technologies needed to apply the Directive. The Commission supported this amendment. The Group rejected this amendment finding it superfluous and in any case too binding.

Amendment 5 (1. and 2.part) on recital 19 and amendment 9 (2.part) (legal persons)

These amendments aim to restrict the possibility for Member States to limit certain provisions to natural persons. The Commission rejected both amendments and was supported by the Group.

Amendment 6 on recital 25 (Procedure for the revision of the Annex)

This amendment aims to emphasise that any substantial changes to the Annex must be introduced in accordance with Article 100a of the Treaty. Both the Commission and all the delegations, except UK, supported this amendment.

Amendment 7 on article 5 (derogations to confidentiality)

The amendment introduces a cross reference to article 14(1). The Commission supported the amendment since it does not change the substance of the Directive. There was a divergence of views in the Group on this amendment, several delegations fearing that the cross reference could limit the scope of derogations.
Amendment 8 on article 9 (elimination of the calling line identification)

This amendment calls only for drafting changes for the common position; however, the Commission and the Group preferred to maintain the common position text.

Amendment 9 (1.part) (the right to not enter in a directory free of charge)

In this amendment the Parliament requests that subscribers can ask not to be entered in a directory free of charge. Apart from F and GR, all delegations could accept this amendment.

Amendment 10 (ANNEX)

In this amendment the Parliament wishes to add a new indent 5a to the ANNEX which specifies what information a telecommunications organisation has to keep confidential. The Group and the Commission could accept this amendment.
"I/A" ITEM NOTE

from: General Secretariat of the Council
to: Permanent Representatives Committee (Part 1)/Council

No. prev. doc.: 5630/97 ECO 22 CODEC 52
No. Cion prop.: 7966/94 ECO 156

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 telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks – Convening of the Conciliation Committee

1. On 27 July 1990 the Commission sent the Council a 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 telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (1). This was followed by an amended proposal submitted on 14 June 1994 (2).


The Economic and Social Committee delivered its Opinion on 24 April 1991 (4).

(1) OJ No C 277, 5.11.1990.
(2) OJ No C 200, 22. 7.1994.
2. The Council adopted its common position on 12 September 1996 (⁵).


4. The European Parliament's amendments were examined by the Working Party on Economic Questions (Telecommunications) at its meeting on 30 January 1997. It was found that not all the amendments could be approved by the Member States (⁷).


6. The Permanent Representatives Committee is therefore invited to suggest that, when taking the "A" items on the agenda for a meeting in the near future, the Council should decide not to adopt the act as amended by the European Parliament but to convene a meeting of the Conciliation Committee in accordance with Article 189b(3) of the TEC and approve the draft letter annexed to this note.

---

(⁵) OJ No C 315, 24.10.1996.
(⁶) 5429/97 CODEC 36 ECO 14.
(⁷) 5630/97 ECO 22 CODEC 52.
(⁸) 6500/97 ECO 63 CODEC 139.
DRAFT LETTER

COUNCIL
OF THE
EUROPEAN UNION

Brussels,

Mr J.M. GIL-ROBLES
President of the European Parliament
rue Belliard 97/113
1040 BRUSSELS

Sir,

I wish to inform you that Council has been unable to approve all the European Parliament's amendments and therefore cannot adopt 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 telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (00/0288 (COD)).

The Conciliation Committee will consequently be convened in accordance with Article 189b(3) of the Treaty.

Yours faithfully,

A. BOIXAREU
Director-General
COVER NOTE

from  :  Mr D.F. WILLIAMSON, Secretary-General of the European Commission

date of receipt:  6 March 1997

to  :  Mr Jürgen TRUMPF, Secretary-General of the Council of the European Union

Subject:  Opinion of the Commission, pursuant to Article 189b(2)(d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding 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 telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks

  Amending the Commission proposal pursuant to Article 189a(2) of the EC Treaty

Delegations will find attached Commission document COM(97) 94 final 288 (COD).

Encl.: COM(97) 94 final 288 (COD)
REPORT

from: Working Party on Economic Questions (Telecommunications)
on :3 April 1997
to :Permanent Representatives Committee

No. Cion prop.: 6500/97 ECO 63 CODEC 139 COM(97) 94 final - COD 288

Subject: Proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks

I. Introduction

On 16 January 1997, at second reading, the European Parliament proposed eleven amendments to the Council's common position (see 5429/97 CODEC 36 ECO 14).

On 17 March 1997, after noting that it could not approve all the European Parliament's amendments (1), the Council agreed to convene the Conciliation Committee in accordance with Article 189b(3) of the TEC.

At its meeting on 3 April the Working Party on Telecommunications began preparation for conciliation on this matter.

(1) It should be noted that in its Opinion delivered on 7 March, the Commission accepted seven of the amendments (6500/97 ECO 63 CODEC 139).
II. Suggestions by the Working Party on individual amendments (1)

1. Title (amendment 2)

   The Parliament proposed a simplification of the title of the Directive.

   All delegations were able to accept this amendment.

2. Subsidiarity principle (amendment 3)

   Recital 7 of the common position emphasizes the importance of the principle of subsidiarity in this sector; the Parliament, however, takes the view that it is not appropriate to apply this principle.

   As a compromise, the President suggested deleting the reference to the principle of subsidiarity. Although this suggestion was favourably received by B, by the Cion and, in principle, by UK, a number of delegations (DK/D/F/S/A) preferred to maintain the text of the common position.

   The Working Party therefore advocates adhering to the text of the Common Position at this stage.

3. Development of the technologies required for proper application of the Directive (amendment 4)

   The parliamentary amendment introduces a new recital intended to promote cooperation between all the parties concerned (Member States, service providers, users and Community Institutions) in order to speed up development of these technologies.

   The Working Party accepted this amendment, but reworded it slightly in order to make it more flexible. (See text of right-hand column on page 7 of the Annex).

(1) See also the texts set out in three columns in the Annex.
4. **Directories of subscribers and protection of the privacy of natural persons or the legitimate interests of legal persons** (amendment 5)

Recital 14 of the common position emphasizes that the subscriber must be able to determine the extent to which his personal data may be published in a directory; however, it allows the Member States to limit such protection to subscribers who are natural persons.

The Parliament's amendment is intended to restrict this option by making it compulsory for legal persons to appear in the directory, to comply with the public's right to be informed.

**The Working Party** advocates adhering at this stage to the text of the common position, which it feels is sufficiently flexible to take account of the case of legal persons.

5. **Unsolicited calls** (amendments on which a separate vote was taken and which relate to recital 20 and to Article 12(3))

The common position provides for the protection of subscribers against any violation of their privacy by unsolicited calls or faxes, but allows the Member States to limit such protection to those subscribers who are natural persons. The Parliament was not in favour of differentiated treatment for legal persons, and proposed that this option for limitation should be abandoned.

**The Working Party** advocates adhering to the text of the common position.

It should be noted, however, that **UK** suggested aligning Article 13(3) of the common position on the equivalent provision of the "distance selling" Directive, replacing the concept of "subscribers who are natural persons" by "subscribers who are persons acting outside their trade, business or profession".

6. **Technical adaptation of the Annex** (amendment 6)

The Annex to the common position contains an exhaustive list of data which may be processed for establishing subscribers' invoices. The list may be subject to technical adaptation by the committee set up by Article 31 of the general Directive on data protection. The parliamentary amendment emphasizes that recourse may not be had to this procedure for changes of substance.

**The Working Party** suggests retaining the principle of the Parliament's amendment, but in a different wording (see text in the right-hand column on page 9).
7. Confidentiality of communications (amendment 7)

Article 5, which guarantees the right to confidentiality of communications, prohibits in particular listening, tapping or storage of communications by any persons other than users "except when legally authorized". By way of clarification, Parliament is proposing the addition of a cross-reference to Article 14(1), which already sets out the extent to which exceptions may be made to the rights provided for in Article 5.

The Working Party proposes accepting this cross-reference while pointing out either in a recital or in a footnote to Article 5 that Article 5 does not prohibit recordings made for the purpose of providing evidence of a commercial transaction (this clarification refers in particular to stock market operations). (See text in the right-hand column on page 10). However, the UK delegation maintained a reservation on this reference.

8. Implementation in the Member States of elimination of the presentation of the calling line identification (amendment 8)

The Working Party did not retain the text proposed by the Parliament but nevertheless did suggest an amendment intended to meet the Parliament's concerns (see page 10 of the Annex).

9. The right not to be listed in the directories free of charge (amendment 9)

As the Parliament attaches importance to the principle that the right not to be listed in a directory should be free of charge, it proposed the deletion of Article 11(2) (which authorizes Member States to allow operators to require a payment for the exercise of this right to privacy).

The F and EL delegations, supported by UK, opposed deletion of the option provided for in the common position.

10. Date of the call/service (amendment 10)

The Working Party accepted the addition of this data to the list in the Annex to the Directive, as proposed by the Parliament.
<table>
<thead>
<tr>
<th>Common Position</th>
<th>EP Amendment</th>
<th>Possible compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amendment 2</strong></td>
<td><strong>Title</strong></td>
<td></td>
</tr>
<tr>
<td>Common Position</td>
<td>EP Amendment</td>
<td>Possible compromise</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Amendment 3</strong>&lt;br&gt;Recital 7&lt;br&gt;(principe of subsidiarity)</td>
<td>(7) Whereas legal, regulatory, and technical provisions adopted by the member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objectives set out in Article 8a of the Treaty; whereas the harmonization pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;</td>
<td>C.P. Text</td>
</tr>
</tbody>
</table>
Amendment 4
Recital 7a (new)
(cooperation to develop technologies)

(7a) Whereas the Member States, providers and users concerned, together with the competent Community bodies, must cooperate in introducing and developing the relevant technologies needed to apply the guarantees provided for by the provisions of this Directive;

(7a) Whereas 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 the provisions of this Directive;

Amendment 5
Recital 19
(Directories and the right to privacy)

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interests of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(19) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interests of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas, with regard to legal persons, exceptions to this general principle, when the legitimate interests of the subscriber run counter to other interests, such as the user’s right to information must be respected;

C.P. Text
<table>
<thead>
<tr>
<th>Common Position</th>
<th>EP Amendment</th>
<th>Possible compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amendment voted separately</td>
<td>Recital 20</td>
<td>(Unsolicited calls and legal persons)</td>
</tr>
</tbody>
</table>

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(20) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes;
(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology;

(25) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology, and bearing in mind that this procedure cannot apply to substantial changes in these categories of data, which may be undertaken only in accordance with the procedure laid down in Article 100a of the Treaty;

... and bearing in mind that this procedure applies solely to specifications necessary to adapt or to changes in market and consumer demand; otherwise the procedure laid down in Article 100a of the Treaty shall apply.
<table>
<thead>
<tr>
<th>Common Position</th>
<th>EP Amendment</th>
<th>Possible compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amendment 7</strong></td>
<td><strong>Article 5</strong></td>
<td><strong>(Confidentiality of communications)</strong></td>
</tr>
<tr>
<td>(都能做出)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, taping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.</td>
<td>Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, taping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with article 14(1).</td>
<td>Parliament amendment accepted with the following clarification to be inserted either in recital no 14 or in a footnote under Article 5. &quot;The second sentence of Article 5 does not concern taping by users concerned, or on their behalf, and therefore does not prevent the taping of communications for the purpose of providing evidence of a given commercial transaction and the content thereof&quot;.</td>
</tr>
</tbody>
</table>

<p>| <strong>Amendment 8</strong> | <strong>Article 9, introduction</strong> | <strong>(Elimination of the presentation of the calling line identification)</strong> |
| | | |
| Member States shall ensure that the provider of a public telecommunications network and/or publicly available telecommunications service may override the elimination of presentation of the calling line identification: | Member States shall lay down legal provisions governing the way in which the provider of a publicly available telecommunications service may eliminate presentation of the calling line identification: | Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification: |</p>
<table>
<thead>
<tr>
<th>Common Position</th>
<th>EP Amendment</th>
<th>Possible compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amendment 9</strong></td>
<td>Article 11(2)</td>
<td>(The right not to be listed in the directories free of charge)</td>
</tr>
<tr>
<td>2. Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved is reasonable and does not act as a disincentive to the exercise of this right.</td>
<td>Deleted</td>
<td>To be discussed</td>
</tr>
</tbody>
</table>

**Amendment separately voted**

<table>
<thead>
<tr>
<th>Article 12(3)</th>
<th>(Unsolicited calls and legal persons)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Member States may limit the application of paragraphs 1 and 2 to subscribers who are natural persons.</td>
<td>Deleted</td>
</tr>
</tbody>
</table>

**Amendment 10**

<table>
<thead>
<tr>
<th>ANNEX indent 5a (new)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- date of the call/service</td>
</tr>
</tbody>
</table>
CORRIGENDUM TO REPORT

from: Working Party on Economic Questions (Telecommunications)
on : 3 April 1997
to : Permanent Representatives Committee

No. Cion prop.: 6500/97 ECO 63 CODEC 139 – COM(97) 94 final – COD 288

Subject: Proposal for a Directive of the European Parliament and of the Council concerning the protection of personal data and of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks
= preparation for conciliation between the Council and the European Parliament

On page 9 of the Annex, the right-hand column should read as follows:

"and bearing in mind that this procedure applies solely to specifications necessary to adapt the Annex to new technological developments or to changes in market and consumer demand; otherwise the procedure laid down in Article 100a of the Treaty shall apply."
Objet: Adoption, dans les langues de l'Union européenne, de la directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

1. Le 27 juillet 1990, la Commission a transmis au Conseil une proposition de directive du Parlement européen et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications (1).

Le Parlement européen, en première lecture, a rendu son avis le 11 mars 1992, en adoptant une série d’amendements à la proposition de la Commission (2). Par la suite, la Commission a présenté une proposition modifiée le 14 juin 1994 (3).

Le Comité économique et social a rendu son avis le 24 avril 1991 (4).

(1) JO n° C 277 du 5.11.1990.
(3) JO n° C 200 du 22.7.1994.
(4) JO n° C 159 du 17.6.1991.
2. **Le Conseil** a arrêté le 12 septembre 1996 sa position commune (1).

3. Lors de sa session du 16 janvier 1997, **le Parlement européen** a voté en deuxième lecture 9 amendements à la position commune (2).

4. **La Commission** a transmis au Conseil son avis sur les amendements du Parlement européen le 6 mars 1997 (3).

6. Le 17 mars 1997, le **Conseil** a décidé de ne pas arrêter l'acte tel qu'amendé par le Parlement européen et, par conséquent, de procéder à la convocation du Comité de conciliation conformément à l'article 189 B paragraphe 3 du traité CE.


A l'issue de la conciliation, les coprésidents du Comité de conciliation ont constaté, le 6 novembre 1997, que le Comité était parvenu à un projet commun (PE-CONS 3626/97 ECO 253 CODEC 564).

8. **Le Comité des Représentants permanents** est par conséquent invité à suggérer au Conseil:

- d'adopter, en partie "A" de l'ordre du jour d'une de ses prochaines sessions, dans les langues de l'Union européenne, la décision conformément au projet commun figurant au document PE-CONS 3626/97 ECO 253 CODEC 564;

- de décider d'inscrire au procès-verbal de cette session les déclarations figurant à l'addendum 1 à la présente note.

---

(1) JO no C 315 du 24.10.1996.
(2) JO no C 33 du 3.2.1997, p. 78.
(3) Doc. 6500/97 ECO 63 CODEC 139.
ANNEXE

Déclaration des délégations française et hellénique

La France et la Grèce déclarent que, par coûts encourus par l’opérateur pour l’adaptation et la mise à jour de la liste des abonnés à ne pas faire figurer dans l’annuaire public, il convient d’entendre les coûts des moyens techniques et commerciaux nécessaires pour la fourniture spécifique de ce service, dans les conditions de sécurité strictes qu’implique la protection recherchée par l’abonné à ce service.

Déclaration de la délégation allemande

Deutschland geht bei der Interpretation von Erwägungsgrund 7 zu Artikel 3 dieser Richtlinie entsprechend des Gemeinsamen Standpunktes einer Begründung des Rates (Dok. 8937/1/96 REV 1 ADD 1) davon aus, daß es einem Mitgliedsstaat gestattet wird, auf nichtöffentliche oder nicht öffentlich zugängliche Netze und Dienste seine eigenen nationalen Datenschutzbestimmungen anzuwenden, wobei in jedem Fall die Richtlinie 95/46/EWG für die Verarbeitung personenbezogener Daten im Rahmen derartiger Netze und Dienste gilt.
"I""A" ITEM NOTE

from: General Secretariat of the Council
to: Permanent Representatives Committee (Part I)/Council

No. prev. doc.: 5630/97 ECO 22 CODEC 52
No. Cion prop.: 7966/94 ECO 156

Subject: Adoption, in the official languages of the European Union, of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector


The Economic and Social Committee delivered its Opinion on 24 April 1991 (4).

(1) OJ No C 277, 5.11.1990.
(3) OJ No C 200, 22.7.1994.

3. At its sitting on 16 January 1997 the European Parliament adopted 9 amendments to the common position at second reading.(6).


5. On 17 March 1997 the Council decided not to adopt the act as amended by the European Parliament and consequently to convene the Conciliation Committee in accordance with Article 189b(3) of the TEC.

6. The Conciliation Committee met on 24 September 1997. On 5 November 1997, the co-chairmen of the Conciliation Committee noted via an exchange of letters that agreement had been reached on a compromise text.

At the end of the conciliation procedure the co-chairmen of the Conciliation Committee noted, on 6 November 1997, that the Committee had reached agreement on a joint text (PE-CONS 3626/97 ECO 253 CODEC 564).

7. The Permanent Representatives Committee is therefore requested to suggest that the Council:

   – adopt as an "A" item at a forthcoming meeting, in the official languages of the European Union, the Decision as set out in the joint text in PE-CONS 3626/97 ECO 253 CODEC 564.

   – have the statements in Addendum 1 entered in the minutes of this meeting.

---

(6) OJ No C 33, 3.2.1997, p. 78.
(7) 6500/97 ECO 63 CODEC 139.
ADDENDUM TO THE "I"/"A" ITEM NOTE

from : General Secretariat of the Council 

to : Permanent Representatives Committee (Part I)/Council 

No. prev. doc. : 5630/97 ECO 22 CODEC 52  
No. Com.prop. : 7966/94 ECO 156  

Subject: Adoption, in the official languages of the European Union, of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector

Statement by the French and Greek delegations

France and Greece hereby state that the costs incurred by operators in adapting and updating the list of subscribers to be excluded from the public directory mean the costs of the technical and commercial means required specifically to provide this service under the strict security conditions which the protection sought by subscribers entails.

Statement by the German delegation

Germany interprets recital no 7 re Article 3 of this Directive according to the common position outlined in the statement of the Council's reasons (8937/1/96 REV 1 ADD 1) as meaning that a Member State is allowed to apply its own national data protection provisions to non-public or non-publicly available networks and services, with the proviso that Directive 95/46/EC in any case applies to the processing of personal data in the context of such networks and services.
Statement by the Portuguese delegation

The Portuguese delegation is voting in favour of this Directive, resolutely supports its objectives and recognizes its importance for the protection of citizens of the European Union. However, as it indicated when the Common Position was adopted, it would point out that it might, in the case of Article 3, prove necessary to postpone for technical reasons the implementation of certain provisions, particularly in the case of subscribers having access to analogue networks (even if they are connected to digital exchanges).
DRAFT

MINUTES (*)

of the 2054th meeting of the Council
(Telecommunications)

held in Brussels on 1 December 1997

(*) Information on the final adoption of Council acts which may be released to the public can be found in Addendum 1 to these minutes.
## CONTENTS

1. Adoption of the agenda ........................................................................................................................................... 3

2. Approval of the list of "A" items .......................................................................................................................... 3


4. Proposal for a Council Decision adopting a multiannual Community programme to stimulate the establishment of the Information Society in Europe ............................................................................................................. 5

5. Internet
   (a) Open debate
   (b) Proposal for a Council Decision adopting a multiannual Community action plan to promote safe use of the Internet ............................................................................................................. 5

6. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Ensuring security and trust in electronic communication – Towards a European framework for digital signatures and encryption" ............................................................................................................. 6


8. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: "Strategy and guidelines on the further development of mobile and wireless communications (UMTS)" ...................... 8


10. Green Paper on the regulatory implications of convergence in the telecommunications, audiovisual and information technology sectors ................................................................. 10

11. Other business
    – Contribution from the United Kingdom delegation on the problems posed by the coming of the millennium ........................................................................................................................................... 10
1. **Adoption of the agenda**
   12762/97 OJ/CONS 73 ECO 292

   The Council adopted the above agenda.

2. **Approval of the list of "A" items**
   12763/97 PTS A 71

   The Council approved the "A" items as contained in 12763/97 PTS A 71.

   The document references for **Items 1 and 4** should read as follows:

   **Item 1.**
   12100/1/97 CODEC 594 ECO264 REV 1
   + ADD 1
   PE-CONS 3626/97 ECO 253 CODEC 564
   + COR 1 (fin,s)
   + COR 2

   **Item 4.**
   11540/97 RECH 71 USA 20
   + COR 1 (d)
   + COR 2 (fin)
   + COR 3 (en)
   + COR 4 (gr)
   + COR 5 (s)
   + COR 6 (nl)
   + COR 7 (dk)
   + COR 8 (es)
   + COR 9 (f)
   + COR 10 (i)
   + COR 11 (i)
   12309/97 RECH 93 USA 21
   12311/97 RECH 94 USA 22
   + COR 1 (f)

   Information on Items 1 and 2 of the list will be found in **Addendum I** to these minutes.
– Common position
11166/97 ECO 212 CODEC 503
12750/97 ECO 289 CODEC 660

1. With a view to adopting a common position on this Directive, the Council reached a political agreement on the draft submitted by the Permanent Representatives Committee as set out in 12750/97, subject to the following recital being included:

"Whereas, in the interests of the consumer and taking account of the specific situation of the national market, national regulatory authorities may extend the obligation to provide carrier pre-selection with call-by-call override to organizations operating public telecommunications networks without significant market power, where this does not impose a disproportionate burden on such organizations or create a barrier to entry into the market for new operators."

2. The Council also agreed that it would enter the following statement in the minutes of the meeting at which it adopted the common position as an "A" item after finalization of the text by the Legal/Linguistic Experts:

Re Article 20(2)

"The Commission states that the possibilities for deferment under Article 20(2) would apply in particular to parts of the public telecommunications network which will not have been upgraded yet to a modern digital network standard by the deadlines referred to in Articles 12(5) and 12(7) and where the implementation of number portability and carrier pre-selection with call-by-call override could only be accomplished through intermediate solutions requiring disproportionate investments. In such cases, deferment of the obligations under Article 12(5) and 12(7) will be granted following a request which may cover all such problems within the national network, on the conditions and following the procedures mentioned in Article 20(2), with regard to subscriber lines within those parts of the network, until modernization is completed."
4. **Proposal for a Council Decision adopting a multiannual Community programme to stimulate the establishment of the Information Society in Europe**

   **Adoption**
   
   11421/97 ECO 230  
   11477/97 JUR 349 ECO 233  
   12303/97 ECO 27 + COR 1 (f)  
   12943/96 ECO 376

Without prejudice to a parliamentary scrutiny reservation from the German delegation, the Council arrived at unanimous agreement on this Decision on the basis of the text that had been submitted to it (Annex to 12303/97) and with the entry in Article 4 of a financial reference amount of ECU 25 million for the five-year period (1998-2002).

The Council instructed the Permanent Representatives Committee to arrange for the technical, legal and linguistic finalization of the text so that the Decision could be adopted as an "A" item at a Council meeting in the near future.

5. **Internet**

   **(a) Open debate**
   
   12277/97 ECO 271

   **(b) Proposal for a Council Decision adopting a multiannual Community action plan to promote safe use of the Internet**

   **Presentation by the Commission**

   The Council held an open debate concerning the Internet. In the course of this debate, and after the Commissioner Mr BANGEMANN had presented the proposal for a Council Decision concerning a multiannual Community action plan to promote safe use of the Internet, the Council discussed the subject of "the Internet and schools" on the basis of two questions formulated by the Presidency.

   After the debate, during which all the delegations and the Commission spoke, the President noted the interest shown in this matter by all the speakers and the fact that there was a consensus as to its importance for competitiveness and the need to avoid new forms of exclusion in this area. He also noted, however, that there was disagreement as to how schools’ access to the Internet should be funded: some delegations wanted universal-service obligations to be extended, while others, together with the Commission, were opposed to this; yet others thought that such a development would be premature but that it should be considered.
In conclusion, the President suggested that the Council should return to this matter on a regular basis for the purpose of exchanging information and good practice and reviewing the rules in the light of shared experience.

6. **Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Ensuring security and trust in electronic communication – Towards a European framework for digital signatures and encryption"
   
   – Presentation by the Commission; Council conclusions
   
   11391/97 ECO 229
   12759/97 ECO 290

1. In response to the abovementioned communication, which proposes the setting up of a joint European framework for digital signatures and encryption, the Council adopted the following conclusions:


2. The Council recalls:

   – its Resolution of 21 November 1996 on new policy priorities regarding the Information Society; (²)

   – the Directive 95/46/EC on "the protection of individuals with regard to the processing of personal data and of the free movement of such data" of 24 October 1995 (³), the Directive 97/../EC on the "protection of personal data and of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks" of .... 1997 and the Directive 97/13/EC on "a common framework for general authorizations and individual licences in the field of telecommunications services" of 10 April 1997; (⁴)

   – the Council Resolution of 17 January 1995 on the lawful interception of telecommunications; (⁵)

– the Commission communication entitled "A European Initiative in Electronic Commerce" of 16 April 1997;

– the Ministerial Declaration of the Bonn Conference of 6 and 7 July 1997;

– its conclusions of 13 November 1997 on electronic commerce.

3. The Council notes:

– the increasing importance of cryptographic products and services for business, private life and public services notably with a view to global electronic communication and their socio-economic impact;

– the growth and employment potential of a European industry for cryptographic products and services;

– the importance of safeguarding the functioning of the Internal Market in order to ensure the free circulation and use of cryptographic products and services as well as the development of electronic commerce;

– the need for a world-wide compatible framework for cryptographic products and services.

4. The Council also acknowledges the concerns regarding the use of encrypted communication, which might diminish the capacity of Member States to fight crime and to maintain their national security.

The Council notes the need to discuss the relevant aspects of the Communication also within other formations of the Council, such as the "Justice and Home Affairs" Council to ensure a coordinated approach.

5. The Council notes the need to distinguish between authentication and integrity products and services on the one hand and confidentiality products and services on the other.

6. The Council calls upon the Commission to proceed according to the time-table laid down in the communication on digital signatures and encryption, in particular to propose as soon as possible a Directive of the European Parliament and of the Council on digital signatures.

(6) COM(96) 607 final.
7. The Council notes with interest the willingness of the Danish Government to host an international hearing on digital signatures and encryption in the first part of 1998.


   – Progress report

   8944/97 ECO 138 CODEC 337
   12186/97 ECO 268 CODEC 598
   12287/97 ECO 272 CODEC 612

   The Council noted the progress made on the above Directive, as set out in 12287/97, and asked the Permanent Representatives Committee to press ahead with its work to enable a political agreement to be reached on this dossier at the next meeting of the Telecommunications Council.

8. **Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: "Strategy and guidelines on the further development of mobile and wireless communications (UMTS)"**

   – Presentation by the Commission and exchange of views; Council conclusions

   8805/97 ECO 129
   1532/97 ECO 235
   12765/97 ECO 291

   After hearing the Commissioner Mr BANGEMANN's presentation of this communication, the Council adopted the following conclusions:

   "THE COUNCIL:

   WELCOMES the public consultation carried out by the Commission on UMTS;

   EMPHASIZES the world-wide nature of the UMTS market, the development of which should be an industry-led process that represents both a challenge and an opportunity for the takeoff of a global wireless Information Society;

   NOTES the broad lines of consensus emerging from the consultation with regard to the need to set out urgently an overall strategy providing regulatory certainty for UMTS;
WELCOMES in general the actions recommended by the Commission in its communication on strategy and policy orientations with regard to the further development of mobile and wireless communications (UMTS);

CALLS ON the Commission and the Member States to support work undertaken by CEPT/ERC in respect of UMTS spectrum allocation and by ETSI to develop a common, open and internationally competitive standard and to promote the future UMTS standard in the context of the IMT-2000 standardization process undertaken within the ITU, as well as to undertake the necessary measures to ensure the free circulation of UMTS terminals;

CALLS ON the industry, in particular through the UMTS Forum, to lead the development of UMTS by taking strategic and timely decisions related to UMTS with a view to creating a strong European market for UMTS as a basis for its world-wide development;

CALLS ON the industry to participate actively in the UMTS standardization process within ETSI and support the definition of a common, open and internationally competitive standard, in particular for the UMTS air-interface, to facilitate the coordinated introduction of UMTS in the European Union;

INVITES the Commission to submit by early 1998, a proposal for a European Parliament and Council Decision which would enable orientations to be established on the substance of the issue and will facilitate, within the existing Community legal framework, the early licensing of UMTS services and, if appropriate and on the basis of the existing repartition of competencies, in respect of coordinated allocation of frequencies in the Community and pan-European roaming.”

9. **Communication from the Commission to the European Parliament and the Council on the implementation of the telecommunications regulatory package: first update**
   – Presentation by the Commission
   11389/97 ECO 228

1. The Council took note of this communication, which gives a first update of the situation regarding transposition as at 15 September 1997 and reports that the Commission "is encouraged by the evidence of substantial progress in the transposition of the regulatory package and believes that, if joint efforts continue, the Community will have achieved a major milestone by 1 January 1998".

2. The Council took note of interventions from a number of delegations (including the German, Belgian, Danish, Greek, Italian and Portuguese delegations), which put forward comments and information concerning the progress with transposition that had either been made in the very recent past or would be made between now and 1 January 1998.
10. **Green Paper on the regulatory implications of convergence in the telecommunications, audiovisual and information technology sectors – Presentation by the Commission**

The Council took note of an oral presentation by the Commissioner Mr BANGEMANN of the forthcoming Green Paper mentioned above, which the Commission expected to adopt on 3 December 1997. It also noted the interventions made in this connection by the Italian and Netherlands delegations.

11. **Other business**
   
   **– Contribution from the United Kingdom delegation on the problems posed by the coming of the millennium**
   
   12776/97 ECO 293

   The United Kingdom delegation spoke once again about the problem that arose from the fact that many computer systems and programs would be unable to cope with the change of date at the end of the century.

   Several delegations provided information on the measures that had been taken in their countries to resolve this problem.

   The Commissioner Mr BANGEMANN said that a communication on what the Commission had done so far in this matter would be issued in the near future.
DRAFT MINUTES

Subject: 2374th meeting of the Council (TRANSPORT/TELECOMMUNICATIONS), held in Luxembourg, on 15/16 October 2001
CONTENTS

1. Adoption of the agenda ................................................................. 3
2. Approval of the list of "A" items ...................................................... 3

TELECOMMUNICATIONS

3. Telecoms package (common position on the framework, access, authorisation and universal service Directives) ................................................................. 3
4. Proposal for a Directive on the processing of personal data and the protection of privacy in the electronic communications sector ................................................................. 3
5. Commission communication on network and information security: Proposal for a European policy approach ................................................................. 4
6. Commission communication : eEurope 2001: accessibility of public websites and their content ................................................................. 4
7. Commission communication on IDA II evaluation, accompanied by a proposal for a Decision amending Decision n° 1719/1999/EC on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA) and a proposal for a Decision amending Decision n° 1720/1999/EC adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA) ................................................................. 4
8. Proposal for a Directive amending directive 97/67/EC with regard to further opening to competition of Community postal services ................................................................. 5
1. **Adoption of the agenda**  
doc. 12568/01 OJ/CONS 51 TRANS 151 ECO 268

The Council adopted the above-mentioned agenda.

2. **Approval of the list of "A" items**  
doc. 12601/01 PTS A 53 + COR 1(fi)

The Council approved the "A" items as listed in the above-mentioned document.

**TELECOMMUNICATIONS**

3. **Telecoms package (common positions on the framework, access, authorisation and universal service Directives)**  
   – Presidency briefing

   The Presidency informed the Council regarding its informal, preliminary contacts with Rapporteurs and other interested Members of the European Parliament, undertaken with a view to bringing the positions of the Council and the Parliament closer together and thereby facilitating progress in the second reading. The Council took note of the information provided by the Presidency and asked Coreper to pursue its work actively, together with the European Parliament, with a view to adopting the package as soon as possible.

   – Presidency briefing  
   10961/01 ECO 242 CODEC 616  
   10451/01 ECO 202 CODEC 677  
   10972/01 CODEC 748 ECO 218  
   12741/01 JUR 295 ECO 278 CODEC 1013

The Presidency updated the Council regarding the state of this file. In the light of an exchange of views involving several delegations, the Council invited Coreper to re-examine the file in the light of the forthcoming first reading opinion of the European Parliament, with a view to confirming, as far as possible, the agreement in principle achieved at the Transport/Telecommunications Council of 27/28 June 2001.
5. **Commission communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on network and information security: Proposal for a European policy approach**
   - Policy debate
     9727/01 ECO 175 CAB 18 JAI 54 PESC 218
     12463/01 ECO 264 CAB 22 JAI 111 PESC 377

The Council held a policy debate on the subject of network and information security on the basis of the Commission communication and a short questionnaire put forward by the Presidency. In the light of the recent terrorist events in the United States, the Council underlined the importance it attaches to this issue and encouraged the Presidency to continue to accord it a high priority. In particular the Council invited Coreper to prepare a draft Council Resolution, taking into account the results of the debate, to be submitted for adoption to the Transport/Telecommunications Council planned for 6/7 December 2001.

6. **Commission communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: eEurope 2002: Accessibility of public websites and their content**
   - Commission presentation
     12265/01 ECO 260 SOC 357

The Council took note of the Commission's presentation of the above communication.

7. **Commission communication to the European Parliament and the Council on IDA II evaluation, accompanied by**
   - a proposal for a Decision of the European Parliament and of the Council amending Decision No 1719/1999/EC on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA) and
   - a proposal for a Decision of the European Parliament and of the Council amending Decision No 1720/1999/EC adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA).

Commission presentation
11983/01 ECO 246 CODEC 892

The Council took note of the Commission's presentation of the above communication and accompanying proposals.

- Political agreement
  - Political agreement
  - 10544/01 ECO 219 CODEC 572
  - 7419/01 ECO 83 CODEC 273
  - 12642/01 ECO 273 CODEC 999
  - 12658/01 ECO 274 CODEC 1001

With a view to adopting a common position, the Council reached political agreement on the above file, with the NL delegation voting against the agreement and the FIN delegation abstaining.

The text of the political agreement, together with a joint declaration from A and S and a declaration from F for inclusion in the minutes of the Council adopting the common position can be found in document 12879/01 ECO 280 CODEC 1022.

The Commission indicated its support for the political agreement and its intention to make this support clear to the European Parliament during the second reading. In response to questions from certain delegations, the Commission also clarified:

- that the Commission study provided for in the new Article 7(3) of the text will assess for each Member State whether or not full accomplishment of the internal postal market is compatible with the maintenance of universal service provision; and

- its interpretation that, according to the new Article 27 as drafted in the text agreed, Article 26 as a whole will continue to apply after the eventual lapsing of the Directive on 31st December 2008;

- the reference to "specific characteristics", in the context of Article 7.1 paragraph 4, would concern Luxembourg in the first instance and perhaps other Member States.