

**Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data**

*COM(90) 314 final — SYN 287*

*(Submitted by the Commission on 27 July 1990)*

*(90/C 277/03)*

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,

In cooperation with the European Parliament,

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

- (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 fulfil 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 87/373/EEC <sup>(1)</sup>,

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.

*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, under-

going 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

<sup>(1)</sup> OJ No L 197, 18. 7. 1987, p. 33.

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 II

### 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 fulfil 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 fulfil the obligations provided for in Article 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 10 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.
3. The Working Party on the Protection of Personal Data shall adopt its own rules of procedure.
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 of 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.

---

### **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**

*COM(90) 314 final — SYN 288*

*(Submitted by the Commission on 27 July 1990)*

*(90/C 277/04)*

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 cooperation 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 exhorts 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;

- (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 <sup>(1)</sup>, 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 <sup>(2)</sup>;

- (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) <sup>(3)</sup> <sup>(4)</sup> <sup>(5)</sup>;

- (6) Whereas Commission recommendation 81/679/EEC calls for the adoption and ratification by Member

---

<sup>(1)</sup> OJ No C 257, 4. 10. 1988, p. 1.

<sup>(2)</sup> OJ No C 196, 1. 8. 1989, p. 4.

<sup>(3)</sup> OJ No C 7, 12. 1. 1987, p. 334.

<sup>(4)</sup> OJ No C 12, 16. 1. 1989, p. 69.

<sup>(5)</sup> OJ No C 12, 16. 1. 1989, p. 66.