COMMISSION OF THE EUROPEAN COMMUNITIES

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

COMMISSION 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

Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security

I. 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,[1] 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

---

1 OJ No C 257, 4.10.1988, p. 1; OJ No C 196, 1.8.1989, p. 4; OJ No C 7, 12.1.1987, p. 334; OJ No C 12, 16.1.1989, p. 66; OJ No C 12, 16.1.1989, p. 69.

the point of view of the protection of property and persons which, in the context 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.

SYN 287

PROPOSAL FOR A
COUNCIL DIRECTIVE

CONCERNING THE PROTECTION OF INDIVIDUALS IN RELATION TO THE PROCESSING OF PERSONAL DATA

CONTENTS

SUMMARY

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:
  . 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.
  . 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.
  . 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

<u>An equivalent level of protection in the Community</u>

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 I

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.

g) 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 (rectificaion, 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

decide how such information is forwarded to the data subject. 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(8) 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 a 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 approprate 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.

SYN 287

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 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[1],

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 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 thro 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 15

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 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.

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 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, REGLEMENTAIRES ET ADMINISTRATIVES DES ETATS MEMBRES RELATIVES A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE 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 Etats membres (groupe 4)

   2. Pour le Comité consultatif (Art.30) : représentants des Etats 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. Echéancier 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 éliminerons les distorsions de concurrence dûes 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.

Draft

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.**

SYN 288

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

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 ...".

---

1 Council Recommendation of 22 December 1986 on the coordinated introduction of the Integrated Service Digital Network (ISDN) in the European Community (86/659/EEC).

The ISDN can be considered as a natural evolution of the telephone network. It will allow via a single acce using the existing subscriber line, the transmission of voice (telephony), text, data, and images in the form 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 w submitted up to now by the Commission (COM(88) 589; COM(90) 123).

2 Council Recommendation of 25 June 1987 on the coordinated introduction of public pan-European cellula digital land-based mobile communications in the Community (87/371/EEC, OJ No L 196, 17 July 1987, p. and Council Directive of 25 June 1987 on the frequency bands to be reserved for the coordinated introduc of public pan-European cellular digital land-based mobile communications in the Community (87/372/EEC OJ No L196, 17 July 1987, p. 85), and subsequent proposals by the Commission in the field of public digit mobile communications.

3 Resolution on Council Recommendation 86/659/EEC, OJ No C 7, 12 January 1987, p. 334.

4 Resolution on Posts and Telecommunications, OJ No C 12, 16 January 1989, p. 69 ; resolution on the nee overcome the fragmentation in telecommunications, OJ No C 12, 16 January 1989, p. 66.

The Council in its resolution of 30 June 1988[5], by which it adopted the principles of the Green Paper on the development of the common market for telecommunications services and equipment[6] and gave its general support to the objectives of the action programme set out in the communication of 9 February 1988[7] 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[8], 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[9].

---

5 Council Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (OJ No C 257, p. 1).

6 COM(87) 290.

7 Towards a competitive Community-wide telecommunications market in 1992: Implementing the Green Pa 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 C196, 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[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[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"[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.

---

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.

11 See Council Recommendations 86/659/EEC and 87/371/EEC, footnotes 1 and 2 above.

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[13].

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[14], and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and telecommunications[15], 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.

---

14 COM(89)289 - SYN 204, 27.7.1989.

15 OJ No L 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.

SYN 288

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[1];

In co-operation with the European Parliament [2];

Having regard to the opinion of the Economic and Social Committee [3];

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;

---

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 [4] 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];

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) [6,7,8];

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 .... [9] 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.

---

4 OJ No C 257, 4.10.1988, p. 1.

5 OJ No C 196, 1.8.1989, p.4.

6 OJ No C 7, 12.1.1987, p.334.

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, i 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 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 fie 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 identif 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 the 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[10] which lays down a procedure for the provision of information in the field of technical standards and regulations.

[10] OJ No L 109, 26.4.1983, p.8.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Council Directive .....EEC ... [on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity][11], and Council Decision 87/95/EEC of 22nd December 1986 on standardisation in the field of information technology and telecommunications[12].

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 C

[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 Diective 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

FICHE FINANCIERE

PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLICS, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES 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 Etats 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 : 56.160- *

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 Etats 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 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 certains secteurs.

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

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[1]. 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-à-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 competitivity 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 there 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 compris 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. Action Line I - Development of an Information Security Strategy Framework

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. Action Line II - Information Security Requirements

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. Action Line IV - Specification, standardisation and Verification for Information Security

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 (eg. 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. Action Line VI - Information Security Provisions

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 pre-requisite 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;

FINANCIAL STATEMENT

Information Security (INFOSEC)
Preparatory Action

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 in 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):

From the Budget of the Communities:	12.0
From the other sectors at the national level:	0.0
TOTAL	12.0

5.0.1 Multi-annual schedule (in MioECU):

	Commitment Appropriations	Payment Appropriations
1991	6	4
1992	6	6
1993	-	2
	12	12

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 proposals, re-consultation 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 fives the indicative breakdown over the various categories of expenditure (in MioECU):

			1991	1992
5.0.2	a)		4,823	4,100
5.0.2	b)	in total	1,177	1,900
of which		Experts	*0,400*	*0,600*
		Other operational expenditure	*0,500*	*0,725*
		Infrastructure	*0,050*	*0,100*
		Information and publication	*0.050*	*0,100*
		Statutory staff	*0,177*	*0,375*

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.

7. 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.

8. 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.