PROPOSAL FOR A
COUNCIL DIRECTIVE

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

Explanatory memorandum

I. Introduction

II. The need for protection in the Community

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

- Consequences for the Community

III. The approach adopted

- An equivalent level of protection in the Community

- A high level of protection

IV. Discussion of the provisions

This proposal for a directive is aimed at establishing an equivalent, high level of protection in all the Member States of the Community in order to remove the obstacles to the data exchanges that are necessary if the internal market is to function. To that end, the principles set forth in the draft proposal for a directive must be underwritten by the Member States. Those principles relate to the conditions under which the processing of personal data is lawful, the rights of the data subject (right to information, right of access, right to rectification, right of opposition, etc.), the requisite data quality (data must be accurate, collected fairly, stored for specified and lawful purposes, etc.) and the setting-up of a Working Party on the Protection of Personal Data to advise the Commission on data protection issues. The draft proposal for a directive covers both the private sector and those activities of the public sector which fall within the scope of Community law. Since every individual will enjoy in each Member State an equivalent, high level of protection in respect of the processing of personal data, the Member States will no longer be able to restrict the flow of such data in the Community on grounds of the protection of the data subject.
1. 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 23 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, 3.5.1978, p. 27; OJ No C 140, 5.8.1979, 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 telecommunication 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

An equivalent level of protection in the Community

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

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

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

A high level of protection

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

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

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

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

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

IV. DISCUSSION OF THE PROVISIONS

CHAPTER 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 reprocessed 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 services 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 15

Principles

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

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

Article 6

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

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

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

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

Article 7

Obligation to notify the supervisory authority

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

CHAPTER III

Lawfulness of processing in the private sector

Article 8

Principles

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

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

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

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

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

Article 9

Obligation to inform the data subject

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

Article 10

Special exceptions to the obligation to inform the data subject

This article authorizes Member States to provide in their law that, where major practical difficulties, overriding legitimate interests of the controller of the file or a similar interest of a third party stand in the way of informing the data subject, the supervisory authority may, within the limits of the law authorizing it to do so, at the request of the controller of the file authorize a derogation from the obligation to inform the data subject. The supervisory authority may, specify the terms of the derogation and decide to inform the data subject itself.

The case of major practical difficulties covers, for example, data relating to persons whose home address is not known.
Article 11
Obligation to notify the supervisory authority

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

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

CHAPTER IV

Rights of data subjects

Article 12
Informed consent

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

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

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

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

Article 13

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

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

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

The fair and lawful collection of personal data presupposes that the data subject makes his decision whether or not to disclose data relating to him
to the collector 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 16(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 16(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 10), 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 18

Principles

Article 18 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 18(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 18(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 classifies 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 13

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

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

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

Article 18(4) assigns responsibility for compliance with the obligations laid down by Article 18(1) to (3). The persons who - de facto or by contract - control the operations relating to a data file are also responsible for ensuring compliance with the data security requirements. Those to whom this rule applies are, as the case may be, the controller of the file, the user having access via on-line data retrieval and data processing service bureaux performing data processing operations on behalf of the controller of the file.
Finally, Article 13(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 26

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.