COMMISSION OF THE EUROPEAN COMMUNITIES

COM(92) 422 final - SYN 287

Brussels, 15 October 1992

Amended proposal for a
COUNCIL DIRECTIVE

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

---

(presented by the Commission pursuant to Article 149(3) of the EEC Treaty)

EXPLANATORY MEMORANDUM

INTRODUCTION

On 18 July 1990 the Commission sent the Council a set of proposals, including two directives and a decision, which were aimed at facilitating the free movement of data in the Community; they sought to do this by ensuring a high level of protection for individuals with regard to the processing of personal data and by tightening the security of data processing with particular consideration for the development of open telecommunications networks.

The Economic and Social Committee delivered its opinion on the proposals on 24 April 1991 (OJ No C 159, 17 June 1991).

Parliament was consulted under the cooperation procedure, and its committees studied the proposals in detail. On 10 February 1992 Parliament considered the report of the Committee on Legal Affairs and Citizens' Rights (the rapporteur was Mr Hoon), and on 11 March, virtually unanimously, Parliament approved the proposals subject to numerous amendments.

On 31 March the Council adopted the proposal for a Decision in the field of security information systems (OJ No L 123, 8 May 1992).

The amended proposal put forward here is intended to take account of Parliament's opinion.

A. Main amendments

1. The approach to protection

The amended proposal makes two major changes at Parliament's request:

- it drops the formal distinction between the rules applying in the public sector and the rules applying in the private sector;

- it expands the provisions on the procedures for notification to the supervisory authority and on codes of conduct.

The amendments have the advantage of making it clear that the protection provided is the same in both the public and the private sectors.

They also help to avoid excessive bureaucracy and make for greater convergence and equivalence between the methods used to ensure effective protection in the Member States, by clarifying the notification procedures and the terms of reference of the independent supervisory authorities in the light of the degree of danger which the processing of personal data may represent for the rights and freedoms of data subjects.

2. Concepts and definitions

Parliament suggested that the concept of a "file" should be dropped, on the grounds that it was outdated and irrelevant given the development of automation and telecommunications, and that the collection of data should be included among the operations which would constitute "processing" of personal data; after considering Parliament's amendments the Commission is now proposing that the subject-matter of the rules should in fact be the processing of personal data. This change has two advantages: the principles of protection laid down by the Directive are not dependent on a particular technology or form of organization; and the concept of the processing of data allows a general approach to be taken, with attention focusing on the data used and the whole sequence of operations carried out in the light of the objective in view.

The Commission nevertheless considers it necessary to retain and clarify the concept of a "file", so that where processing is not automated the scope of the Directive can be restricted to personal data which are entered or intended for entry in such files.

Lastly, the proposal now supplies a definition of the "third party" to whom personal data are disclosed.

3. Scope and specific exemptions

The following amendments are proposed in response to Parliament's concerns. Their purpose is to guarantee and to reconcile the rights and freedoms involved, so as to ensure that data can move freely.

(i) The initial proposal would have excluded processing carried out by non-profit-making organizations from the scope of the Directive; this was criticized as inappropriate, and in line with certain of Parliament's amendments concerning the processing of sensitive data it is now proposed that processing of this kind should fall within the scope of the Directive, with provision for special exemption from the obligation to notify where necessary in order to guarantee freedom of opinion.

(ii) Where processing is carried out for purposes of journalism it is proposed that Member States should be required, rather than merely permitted, to lay down the exemptions necessary to reconcile the right of privacy with freedom of speech.

(iii) Processing may involve no particular danger, and be carried out for example to satisfy a legal obligation, and it is proposed that there should be an exemption from the obligation to notify in such cases.

4. Third countries

The rule intended to prevent the Community rules from being circumvented in the course of transfers of data to non-Community countries takes the form of a ban on the transfer of data to countries which do not provide an adequate level of protection; this has now been clarified in order to remove any ambiguity as to the purpose pursued. Tests by which adequacy is to be measured have been added. Exceptions to the principle have also been laid down in a limited number of cases where particular circumstances appear to justify this.

B. Form and content of the amended proposal

The proposal has been restructured in order to take account of the dropping of the formal distinction between the public and private sectors and the expansion of the provisions on notification to the supervisory authority which have already been referred to. The new structure is also intended to provide a plainer exposition of the different components in the protection mechanism. Lastly, it takes account of criticism of redundancy in the initial version. This restructuring of the proposal affects Chapters II to VI of the initial proposal; these are now for the most part grouped together in a single Chapter II, which sets out all the general rules on the lawfulness of the processing of personal data, one by one, in a new order. The structure of Chapters I, VII and after have not been changed.

The new Chapter II is divided into sections, which lay down the principles which are to govern the design and implementation of processing operations carried out on personal data (Sections I, II and III), the data subject's rights of information, access and objection (Sections IV, V and VI), obligations regarding security (Section VII), and procedures for notification to supervisory authorities (Section 8).

Section I sets out principles governing the quality of data to be processed; the principles are common to the laws of all Member States, and derive from Council of Europe Convention No 108. Section I corresponds to Article 16 in the initial proposal. The inclusion of data collection in the definition of processing, which was asked for by Parliament has made a few drafting changes necessary. Parliament's request that data should be storable for academic purposes has also been met here.

One of the principles listed in Section I, that data must be processed for a legitimate purpose, is clarified in Section II, which deals with the grounds for processing data. This Section reproduces and clarifies the exhaustive list of the various circumstances in which processing may be carried out, and gives it a general character. The list permits processing where the data subject has consented, or where a contract with the data subject makes it necessary, or to comply with a legal obligation, etc., and ends with a clause allowing private interests to be weighed against others. This balance-of-interest clause is likely to concern very different kinds of processing, such as direct-mail marketing and the use of data which are already a matter of public record; Member States are to weigh the balance of interest in accordance with procedures which they are to establish taking account in particular of the general principles in Section I and of the rights of data subjects.

Section III lays down specific rules governing types of processing which might interfere with fundamental freedoms. In line with the Convention already referred to and with Parliament's opinion, which has been followed in part here, these rules provide for stricter protection where the data to be processed are sensitive, that is to say relating in particular to freedom of opinion. These provisions correspond to Article 17 in the original proposal. They take account of Parliament's suggestions particularly regarding processing carried out by associations of a political or trade-union character. In the amended proposal such processing falls within the scope of the Directive, which allows the rights of individuals to be guaranteed in this respect and the free movement of such data to be ensured. Section 3 also sets out the rules already referred to regarding processing for purposes of journalism, which are intended to reconcile the two fundamental freedoms of privacy and freedom of expression.

Section IV deals with the obligations of the controller to inform the data subject of the processing which takes place. The obligations are intended to ensure transparency in processing, and thus to underpin the principles of the fair processing of data which are laid down in the Council of Europe Convention, and which have already been referred to in Section I. Section IV corresponds to what were Chapters II, III and IV in the original version; the wording has been altered particularly in order to remove any danger that it might be interpreted as requiring more information than is necessary.

Section V concerns the data subject's right of access to data concerning him and his right to have it rectified. It corresponds to certain provisions of Chapter IV in the original proposal, and takes over Parliament's amendments, which generally broaden the scope of this entitlement (particularly the data subject's entitlement to be told the source of the data being processed and the reasoning applied in any automatic processing operation the outcome of which is invoked against him). The amended provisions also take account of Parliament's request that the circumstances in which the exercise of the right of access may be restricted should be extended to the private sector on the same terms as the public sector.

Section VI concerns the data subject's right to object on legitimate grounds. It corresponds to the relevant provisions of Chapter III and IV in the initial proposal. The requirement that data subjects must be offered the possibility of opting out of the disclosure of data to third parties with a view to canvassing is laid down here.

Section VII reproduces the rules on security which were set out in Chapter V of the initial proposal, with a few drafting changes.

Section VIII develops the original rules on notification. The selective system proposed is for the most part taken over from Parliament's amendments; it seeks to ensure that processing is transparent and that its purposes are stated, while directing supervisory authorities' attention to types of processing which deserve special attention because of the dangers they involve. The system is based on the approach that all processing must be notified to the supervisory authority once it is wholly or partly automatic, although one notification may refer to a set of processing operations whose purposes are linked from the point of view of the controller or in terms of the data subject. On the basis of their experience it is proposed that Member States may take measures to exempt from the notification requirement processing operations which do not represent any danger to the data subjects' rights and freedoms; they may also simplify the requirement. Measures of this kind are to describe the processing operations covered and where appropriate the circumstances in which they are to be carried out. It is also proposed that the supervisory authority may be empowered to examine notified processing operations before they are carried out.

Chapter III groups together the provisions of Chapters IV and VII of the initial proposal, dealing with the remedies open to data subjects, liability, and penalties. These provisions have been amended to take account of Parliament's opinion.

Chapter IV deals with transfers of personal data to non-member countries. It corresponds to Chapter VIII of the initial proposal. It has been amended in the way already indicated, and leaves scope for the Community to develop a common policy on the subject.

Chapter V is concerned with codes of conduct. It corresponds to the relevant provisions in the original Chapter VI. It follows Parliament's opinion on the involvement of the independent supervisory authority in the drawing up of codes of conduct. It also allows Member States to give trade associations a role in the application of the legislation by allowing them to participate in drawing up national codes of conduct.

Chapter VI deals with the national supervisory authority and the Working Party which is to help to ensure that the national provisions adopted pursuant to the Directive are uniformly applied and to advise the Commission. The investigative powers of the national authorities are clarified, as Parliament had hoped. The composition of the Working Party has been left unchanged, in order to guarantee its independence. For the same reason it is proposed that the Working Party should elect its own chairman. The circumstances in which it is to be consulted by the Commission are spelt out.

Chapter VII concerns the executive powers which the Council is asked to confer on the Commission. Here the Commission maintains its initial proposal, contrary to Parliament's opinion. The Commission takes the view that technical measures will be needed in order to apply the Directive, given the extent and the highly technical character of the field of personal data protection.

Final provisions: in response to Parliament's request the proposal now provides that after the date by which Member States must comply with the Directive there is to be a further period of three years in which the new requirements need not apply to situations already existing.

COMMENTARY ON THE TITLE AND RECITALS

TITLE

Two points have been clarified in the title:

- the words "and on the free movement of such data" have been added in order to emphasize that the proposal is aimed at establishing a working single market, on the basis of a harmonization of legislation which ensures the protection of individuals;

- to eliminate any ambiguity as to the scope of the proposal it is made clear in the title that it is individuals who are to be protected, and not all persons both natural and legal (this change does not affect the English version).

RECITALS

The Commission has amended the recitals in order to take account of the changes to the substantive provisions.

The following specific remarks may also be made:

- Recital No 2 is drawn from Parliament's opinion (amendment No 9), and seeks to point out the advantages of automatic data processing systems provided they respect individual rights and freedoms;

- it appeared preferable to place the recital referring to the Council of Europe Convention among those describing the requirements of a Community policy on the subject, because the Directive embodies the principles set out in the Convention; this recital has now become recital No 10; the same recital was previously placed among those dealing with transfers of data to non-member countries, as recital No 22;

- a new recital No 14 has been inserted which seeks briefly to summarize the principles of protection referred to in the succeeding recitals;

- the changes in the new recital No 4 and recital No 5 are intended to amplify the description of the facts leading up to a Community initiative, the justification for which is then spelt out in recitals Nos 7 and 8.

COMMENTARY ON THE ARTICLES

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

Article 1 defines the object of the Directive. The Directive seeks to ensure the free movement of personal data between Member States by providing for a harmonization of national legislation.

(1) Paragraph 1 requires Member States to protect the rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right of privacy (the terminology is based on that of Article 1 of the Council of Europe Convention).

(2) Under the Directive the protection provided is to follow the same lines in all Member States, and will thus be equivalent throughout the Community; and paragraph 2 accordingly prevents Member States from restricting the free flow of data in the fields covered by the Directive on grounds relating to the protection of data subjects.

The proposal thus seeks to reconcile the requirements of the single market with those of data protection, in line with Parliament's wishes (amendment No 10).

Parliament's amendment No 11 has likewise been incorporated into the amended proposal, by enlarging the definition of "processing" in Article 2(a) to include the collection of data.

Article 2

Definitions

This Article defines the main concepts used in the Directive. The definitions are taken from the Council of Europe Convention, but have been adapted and clarified to ensure equivalent protection at a high level in the Community.

(a) "Personal data". The amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual (amendment No 12). A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.). The definition would also cover data such as appearance, voice, fingerprints or genetic characteristics.

"Depersonalized" data are not defined: the term is not used in the Directive. This means that whether or not data are depersonalized no longer depends on the cost of determining the data subject's identity (amendment No 13). However, in the specific case where data are compiled in the form of statistics, it has been considered appropriate to state that they cannot be considered to be personal data where the data subjects can no longer reasonably be identified.

(b) "Processing of personal data" ("processing"). The definition given here is likewise an extensive one, the better to ensure that individuals are protected (amendment No 15), as it covers everything from the collection to the erasure of data, including organization, use, consultation, disclosure by transmission, dissemination or otherwise making available (amendment No 16), comparison and suppression.

(c) "Personal data file" ("file"). This definition, which covers both automatic and non-automatic files, is now clarified. In the case of non-automatic processing it allows the scope of the Directive to be confined to sets of data which are structured so as to facilitate access and searches for data on individuals. Personal data which are not organized so that they can be used with reference to the data subjects themselves are thus excluded. In practice data of this kind do not present the same dangers for individuals, and it is more realistic not to subject them to the same obligations.

To ensure that individuals are properly protected the criteria for access must have the "object or effect" of facilitating the use or comparison of data. This means that the data subject has does not have to prove intention, something which might have made it difficult to apply the national legislation.

The word "comparison" has been preferred to "combination" because it is appropriate both to automatic processing and to files kept on paper.

(d) "Controller". The definition is borrowed from the definition of the "controller of the file" in the Council of Europe Convention.

But as the Directive sets out to regulate the use of data in the light of the object being pursued, it is preferable to speak of the "controller", and to drop any reference to a "file" or to "data".

The controller is the person ultimately reponsible for the choices governing the design and operation of the processing carried out (usually a chief executive of the company), rather than anyone who carries out processing in accordance with the controller's instructions. That is why the definition stipulates that the controller decides the "objective" of the processing. This is in line with Parliament's amendment No 17. The controller may process data himself, or have them processed by members of his staff or by an outside processor, a legally separate person acting on his behalf.

(e) "Processor". This is a useful definition proposed by Parliament (amendment No 18).

(f) "Third party". This definition is taken from one of Parliament's amendments (No 134); it has been reworded in the amended proposal in order to make it clear that third parties do not include the data subject, the controller, or any person authorized to process the data under the controller's direct authority or on his behalf, as is the case with the processor.

Thus persons working for another organization, even if it belongs to the same group or holding company, will generally be third parties.

On the other hand, branches of a bank processing customers' accounts under the direct authority of their headquarters would not be third parties. The same would apply to the employees of insurance companies; in the case of insurance brokers, on the other hand, the position may vary from case to case.

(g) "The data subject's consent". In the initial proposal the definition of a person's consent to the processing of data concerning him was given in Article 12, dealing with the rights of data subjects.

This caused some confusion; some interested parties drew the conclusion that all processing required the prior consent of the data subject, whereas consent was only one of the possible grounds making processing lawful.

It seems more logical, therefore, to put the rules on consent in Article 2, with a few changes of wording so as to cast them in the form of a definition.

The reference to consent being "express" has been removed, lest it be interpreted as requiring written consent (a procedure confined to sensitive data in Article 8 of the amended proposal). It has been replaced by the concept of an "express indication of his wishes", something which may be either oral or in writing.

The amended proposal makes it clear that consent must be "freely given", in cases where pressure might be brought to bear on the data subject (the case of a wage-earner and his employer, for example).

To enable the data subject to make an assessment of the advantages and disadvantages of the processing of data concerning him, and to exercise his rights under Article 13 of the proposal (rectification, erasure and suppression), the consent given must be informed consent. The controller must supply the data subject with the information he needs, such as the name and address of the controller and of his representative if any (see Article 4(2)), the purpose of the processing, the data recorded, etc.

The data subject's consent must be "specific", meaning that it must relate to a particular data processing operation concerning the data subject carried out by a particular controller and for particular purposes.

The data subject may withdraw his consent at any time. But this withdrawal has no retrospective effects; otherwise a processing operation which was lawful when carried out might become unlawful retroactively.

Three definitions in the original proposal have been deleted:

- the definition of the supervisory authority, which is covered by Article 32 of the amended proposal;
- the public and private sectors, as the provisions dealing with the two sectors have been merged (Chapter II of the amended proposal).

Article 3

Scope

Paragraph 1 of the amended proposal seeks to accommodate the views of those who as far as data processing is concerned would like to refer only to processing "by automatic means" (because automatic processing does not necessarily require the existence of a file) and of those who are afraid that the Directive might be extended to cover all data stored on paper, whether structured or unstructured.

The amended proposal therefore lays down separate tests for determining the scope of the Directive, depending on whether or not the data are being processed by automatic means: it is to apply to the non-automatic processing of data only if the data form part of a file; on the electronic side, however, the definition does not depend on the presence of a file, and the Directive applies to any automatic processing of data even if they do not form part of a file.

Thus structured personal data are caught by the definition if they are organized in a manual file or by electronic data processing methods.

The provision refers to processing "wholly or partly by automatic means" in order to indicate that a processing operation constitutes a single whole even if only part (such as the index) is computerized.

Paragraph 2 makes two exceptions:

- the first exception concerns processing in the course of an activity which falls outside the scope of Community law (in the secret services for example); the scope of the Directive is defined in terms of the scope of Community law, so that it can evolve with it;

- the second exception concerns the use of data in the course of a purely private activity, such as an electronic diary (amendment No 22);

- no other exceptions are laid down, because if too many types of organization were to be exempted from any obligation the rights of the individuals would no longer be guaranteed: while the rules governing certain types of processing of personal data may well be simplified (see Section VIII in Chapter II, on notification, which makes provision for exemption and simplification), a general exemption is not possible.

The particular problem of associations is dealt with in the Article providing for the exemption of the collection of sensitive data (Article 8 in the amended proposal).

Article 4

National law applicable

This Article lays down the connecting factors which determine which national law is applicable to processing within the scope of the Directive, in order to avoid two possibilities:
- that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;
- that the same processing operation might be governed by the laws of more than one country.

Under the original proposal the place where the file was located was to determine territorial jurisdiction, but this criterion has not been retained in the amended proposal, on the ground that the location of a file or of a processing operation will often be impossible to determine: processing operations may have more than one location and take place in several Member States, particularly in the case of data bases connected to networks, which are becoming increasingly frequent.

Under the amended proposal, therefore, the law applicable is defined by reference to the place of establishment of the controller.

A controller who is not established in the Community, may for the purpose of processing make use of means, whether or not automatic (terminals, questionnaires etc.), which are located in the territory of a Member State, and here the law applicable is to be that of the state on whose territory those means are located. The controller must then designate a representative established in that Member State, who is to be subrogated to the controller's rights and obligations.

In that case it is the representative who will be subject to the obligation to notify (Section VIII of Chapter II); and any information regarding the controller which has to be supplied to data subjects under the Directive will have to be supplemented by information on the controller's representative.

The amended proposal follows Parliament's amendment No 24 in removing the reference to sporadic use, a vague term which would have been open to various interpretations.

The reference to the place of establishment of the controller means that the temporary removal of a file does not affect the law applicable. Article 4(3) of the initial proposal has accordingly been dropped.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

The structure of the amended proposal is different from that of the initial proposal: the new Chapter II groups together all the rules, rights and obligations which determine the lawfulness of processing operations. In line with Parliament's opinion, the provisions on the public and private sectors have been run together.

Article 5

This Article takes over Article 6(2) and Article 8(1) and (3) of the initial proposal. It requires Member States to provide that the processing of personal data is lawful only if carried out in accordance with Chapter II, which forms a whole.

By way of explanation the Article also makes it clear that Member States may in their laws more precisely determine the circumstances in which processing is lawful, always subject to Chapter II. Depending on the particular area they might for example wish to determine the cases in which the interests of the data subject prevail (Article 7(f)), the methods by which information is to be given to data subjects (Section IV), or the way in which the right of objection is to be exercised (Section VI). Such provisions may not stand in the way of the free movement of data within the Community.

SECTION 1

PRINCIPLES RELATING TO DATA QUALITY

Article 6

This Article takes over the thrust of Article 5 of the Council of Europe Convention.

It contains the provisions concerning the fundamental rights of individuals with respect to data processing, and has been put at the beginning of the Chapter dealing with the lawfulness of processing operations. It will be necessary to refer back to this Article to interpret the subsequent Articles in the Chapter.

As compared with the Convention the Article makes several changes intended to adapt the Convention's wording to the definitions in Article 2 of the proposal, particularly the definition of "processing", and also to the scope of the Directive, which unlike the Convention applies both to automatic processing and to non-automatic processing of data contained in files.

Article 6(1)(a) provides that personal data must be processed fairly and lawfully. The "processing" referred to is that defined in Article 2(b), and thus includes collection.

The rule laid down in Article 6(1)(a) excludes the use for example of concealed devices which allow data to be collected surreptitiously and without the knowledge of the data subject, by means of telephone tapping and the like. This provision also prevents controllers from developing and using clandestine processing operations for personal data.

Article 6(1)(b) states the principle of the purpose of the collection of data (whether by automatic or non-automatic means). Personal data may be stored only for specified, explicit and legitimate purposes.

The purpose of the collection of personal data must be "specified", that is to say that the aim of the collection and use of data has to be defined in as precise a fashion as possible. A general or vague definition or description of the purpose of processing operations ("for commercial purposes", for example) would not satisfy the requirement that the purpose be specified.

The purpose must be specified before the data are collected. Where the data are collected from the data subject, Article 11 requires that the purpose must have been determined at the time of collection.

A subsequent change in the purpose of a processing operation will be lawful only to the extent that it is compatible with the initial purpose.

Article 6(1)(b) also obliges the controller to determine the purpose of the storage and recording of data.

Personal data can be stored and used only for a "legitimate" purpose, so that the potential purposes of processing are limited. A processing operation may be designed and performed only for a purpose permitted by the Directive and by the domestic legislation in the Member States.

Article 6(1)(c) states that data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. This rule requires that the nature of the data should correspond to the end in view.

Article 6(1)(d) is closely bound up with Article 6(1)(b) and (c). Data must be accurate and, if necessary, kept up to date. If data are inaccurate or incomplete given the purpose of the file, Article 6(1)(d) provides that they are to be erased or rectified.

Article 6(1)(e) concerns the time for which personal data may be kept. Data may be kept in a form which permits identification of data subjects for no longer than is necessary to achieve the objectives for which the data were recorded.

In some cases, however, where after a certain period a processing operation is no longer needed for its primary function, it may be necessary to store the information, particularly for historical or scientific use. Article 6(1)(e) therefore states that, as Parliament had requested (amendment No 60), Member States may provide for further safeguards for data stored for historical, statistical or scientific use, in order to reconcile on the one hand the principle of the legitimate purpose and the entitlement to have one's past forgotten and on the other hand the requirements of research.

Article 6(2) obliges the controller to ensure that the rules on the quality of data laid down in Article 6(1) are complied with.

SECTION II

PRINCIPLES RELATING TO THE PROCESSING OF DATA

Article 7

Article 7 provides a simplified and restructured statement of the grounds on which personal data may lawfully be processed; in the initial proposal this matter was to be found in Articles 5, 6 and 8.
The distinction between the public and the private sectors has been dropped, as proposed in Parliament's amendments Nos 27, 28 and 29.

There is no longer any specific reference to the processing of data for a purpose other than the original one, a possibility covered in Article 5(1)(b) of the initial proposal, or to the lawful disclosure of personal data, which was treated in Articles 6 and 8(2) of the original proposal. It is felt that the general rule that data must be used in a way compatible with the purpose for which it was collected, laid down in the new Article 6(1)(b), together with the statement of possible grounds for the processing of data, set out in the new Article 7, will be sufficient here.

The criteria which Parliament proposed in its amendments No 30 and 32 have been accepted only in a modified form.

Consent is no longer the main criterion, subject to exceptions; it is now the first of several alternatives (new Article 7(a)).

The reference to a "quasi-contractual relationship" was considered by many sources to be vague and to fall either under the concept of a contract or under that of a legitimate interest (referred to in the new Article 7(f)); and the wording "steps at the request of the data subject preliminary to entering into a contract" has now been used to cover the situation before any contractual relationship is established (new Article 7(b)).

The reference to processing in order to comply with an obligation imposed by national or Community law has been maintained (new Article 7(c)).

The same applies to the new Article 7(e) and in part to Article 7(f).

The new Article 7(d) has been added to provide for cases in which the data subject has a vital interest in having his personal data processed but is not in a position to give his consent (in serious medical cases for example).

Article 7(f) has been drafted partly in response to Parliament's amendment No 32; it expands the initial Article 8(1)(c), and takes into account the fact that there may be legitimate interests at stake other than those of the controller and of the data subject. Article 8(1)(b) of the initial proposal has been deleted, because the Commission has established that in certain cases the "sources generally accessible to the public" to which it referred may in fact include sensitive personal data. In any event the data will usually have been processed for specific purposes, and should not be used for different purposes except in accordance with the other provisions of the Directive.

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

This Article corresponds to the original Article 17.

It is generally accepted that it is not so much the content of data which may endanger privacy as the context in which the data is processed. However, there is a broad consensus among the Member States that certain categories of data do by their nature pose a threat to privacy. Article 8 of the proposed Directive therefore places strict limits on the processing and use of data revealing racial or ethnic origin (which will include information on skin colour); political opinions; religious, philosophical or ethical persuasion, which will include the fact that a person holds no religious belief, as well as information on any activities relating to such a persuasion; trade-union membership; information on the data subject's health, which will include his state of physical and mental health, past, present and future, and any indication of drug or alcohol abuse; and information concerning sexual life. Beliefs besides religious or philosophical beliefs might constitute sensitive data, and the word "ethical" has been added accordingly.

The Article initially proposed has been amended and restructured to take account of points raised by Parliament (amendments Nos 63, 149 and 65).

Paragraph 1 lays down a general ban on the processing of this "sensitive" data - whether by manual or automatic means, a point included in response to Parliament's amendment No 63.

Paragraph 2 provides for a number of exceptions to the general rule:

(i) Rather than requiring "express and written consent, freely given" as a general condition for the processing of sensitive data, subject to exceptions, it is considered preferable to list consent as one of a number of alternative exceptions to the general prohibition on the processing of such data.

(ii) Such data may be processed by foundations or associations of a political, philosophical, religious or trade-union character in the course of their legitimate activities, and on condition that the data relate solely to members of the body and persons who have freely entered into correspondence with it, and are not disclosed to third parties. Processing of this kind is not to be subject to the obligation to notify imposed in section VIII of the amended proposal, something Parliament had requested in its amendment No 149.

(iii) Processing may be carried out in circumstances where there is manifestly no infringement of the data subject's privacy or freedoms. Examples of processing of this kind would be the assembly of data of a political nature concerning a public representative, or the compilation of lists of persons to be approached for opinion poll purposes over a short period of time, under strict security measures.

Paragraph 3 reproduces Article 17(2) of the initial proposal, permitting exemptions on "important public interest grounds." An exemption should be given, for example, to international human rights organizations which require such data for their work, provided they can offer suitable safeguards.

Parliament felt that data concerning criminal convictions should be held only by judicial authorities (amendment No 65), and this point has been accepted in part in paragraph 4. Such data could be held by judicial and law enforcement authorities, but also by the persons directly concerned with those convictions or by their representatives. Given the particularly sensitive nature of such data any exemptions would have to be laid down in legislation, with suitable safeguards specified.

Parliament proposed a new Article 3a requiring Member States to enact the conditions under which a national identification number, where such a number exists, or other identifier of a general nature might be used (amendment No 65); this amendment has been accepted, and incorporated as paragraph 5.

Article 9

Processing of personal data and freedom of expression

This Article corresponds to the initial Article 19. There is a danger of conflict between the fundamental rights of individuals, particularly the right to privacy, and the freedom of expression, and the Member States are here required to lay down exemptions from the requirements of the Directive for the press and audiovisual media. The approach adopted lays emphasis on the obligation to balance the interests involved in granting exemptions. Account may be taken for example of the availability 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.

To ensure a measure of harmonization it is now to be obligatory for the Member States to grant exemptions for the press, the audiovisual media, and - an addition to the original text - journalists. Such exemption would be possible only in respect of processing for journalistic purposes. The term "journalists" is intended to include photojournalists and writers such as biographers.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Section IV brings together all the provisions concerning the information to be given to the data subject which were to be found loosely scattered in the initial proposal (initial Articles 9, 13 and 14(3)).

Article 10

The existence of a processing operation

This Article corresponds to the initial Article 14(3), providing for the right "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".

The following changes have been made.

It is specified that this entitlement may be exercised on request. "Habitual residence, headquarters or place of business of the controller of the file" have been replaced by the "name and address of the controller or his representative", as these are felt to be sufficient particulars to allow the data subject to exercise his rights. The data subject is now also entitled to know the categories of data concerned and the identity of any third parties.

Member States may restrict this entitlement in accordance with Article 14(1) on grounds of national security, defence, public safety, etc.).

Article 11

Collection from the data subject

This Article grants specific information rights to a data subject from whom personal data are collected; it corresponds to the initial Article 13.

If personal data are to be collected fairly and lawfully the data subject must be able to decide whether or not to disclose data relating to him in full knowledge of the purposes of the processing, the existence or otherwise of a legal obligation to disclose the data, and the consequences for him if he fails to reply. To ensure that he can defend his rights and monitor the use of data relating to him he should also be informed of his rights of access and rectification, and given details of the recipients of the data.

The following changes have been made:

(i) The title now specifies that it is when data are collected from the data subject that the Article applies.

(ii) This is confirmed in paragraph 1, which makes it clear that what is involved is not just a right enjoyed by the data subject, to be exercised on request, but an obligation on the controller whenever personal data are collected from data subjects. How this is to be put into practice will depend on the particular circumstances in which the data are collected.

(iii) Like Article 13(2) in the initial proposal, the new Article 11(2) empowers the Member States to restrict this duty to inform on grounds of an overriding general interest. The information referred to in paragraph 1 would not have to be supplied where that would hinder or prevent the performance of a monitoring or inspection function by a public authority or would hinder or prevent the maintenance of public order.

Article 12

Disclosure to a third party

This Article corresponds to Article 9 of the initial proposal. To enable the data subject to exercise his rights, paragraph 1 requires the controller to inform the data subject that data relating to him are being disclosed. This will enable the data subject to exercise his right of access or to object to a continuation of the processing in question.

Parliament's amendment No 35 has been accepted to the extent that it referred to those provisions of amendment No 32 which have been accepted. The Article 8(2)(a) to which Article 35 referred corresponds to the Article 7(c) now referred to in Article 13; Article 8(2)(e) corresponds to the new Article 7(b), and Article 8(2)(g) partly corresponds to the new Article 7(f).

The data subject's right to object to processing operations, which include disclosure, is dealt with in Section VI, Articles 15 and 16. The amended Article 15 takes over the spirit of paragraph 3 of Parliament's amendment No 35, omitting the concept of "agent", which was felt to be unnecessary and confusing.

In the initial text the obligation to supply information when data are disclosed essentially applied to the private sector, but the amended proposal makes no distinction between the public and private sectors.

No reference is made to "on-line consultation", since this is covered by the word "disclosure". The obligation to inform is not to apply:

- where disclosure is necessary in order to safeguard the data subject's vital interests (it may be impossible to inform him, or may be contrary to his interests to do so);
- where the data subject has already been informed that the data are to be disclosed or may be disclosed;
- where disclosure is required by legislation making an exception to the obligation to inform;
- where the data are disclosed for one of the reasons listed in Article 14(1) (national security, defence, public safety, etc.).

It is felt that the data subject should be informed not only of the purpose of the processing, the type of data concerned, and the name and address of the controller or his representative, but also of the recipients or categories of recipients, or the existence of rights of access, rectification and objection.

Article 12(3) of the amended proposal corresponds to Article 10 of the initial version, which made a special exception to the obligation to inform the data subject where this proved impossible or would involve a disproportionate effort, or conflicted with the overriding legitimate interests of the controller of the file or a similar interest of a third party. It is now added that a supervisory authority granting an exemption of this kind must lay down any suitable safeguards; this is to ensure that the data subject's rights and freedoms are not unduly injured by a lack of information.

The power to exempt from the obligation to inform should be exercised, for example, in respect of human rights and humanitarian organizations, so that their legitimate work is not unduly hindered.

Article 13

Right of access

This Article includes those provisions of the initial Article 14 which concerned the data subject's right of access to his own personal data and the related right to obtain rectification, erasure or blocking of such data (the original paragraphs 4, 5 and 7). Like Article 14(4) of the initial text, the amended Article 13(1) confers on the data subject the right to obtain, at reasonable intervals and without excessive delay or expense, confirmation of the existence of personal data relating to him and communication of such data to him in an intelligible form.

It is left to the Member States to specify how such information is to be forwarded to the data subject, in order to ensure that the data are disclosed to the right person, for example, or in order to facilitate matters both for the controller and for the data subject where several processing operations are concerned, especially in the case of manual files. It is also left to the domestic law of the Member States to determine the meaning of the term "reasonable intervals". Taking account of the interests both of the data subject and of the controller, the domestic law of the Member States may provide that the controller is entitled to charge a data subject who exercises his right of access, but the amount charged must be no more than the actual cost incurred. The charge must not be excessive.

Article 13(1), corresponding to the old Article 14(4), has been amended in the light of Parliament's amendment No 48, which has been accepted in part. The right of access may be exercised on request. The data subject is to be entitled to obtain information on the source of the data (rather than their "general origin", a term which was felt to be too vague, and consequently to serve no purpose), and general information on their use, rather than information on their "exact use" (a term which was felt to be excessively burdensome and bureaucratic). This provision also allows Member States to make special provision for access to medical data. To avoid exposing the data subject to extreme psychological shock it could be required that such information be provided to him by a medical practitioner.

Article 13(2) has been added in response to Parliament's amendment No 132. It is directed against the misuse of the right of access, against the legitimate interests of the data subject (the example given by Parliament is that the data subject may not be required by any person to exercise his right of access as a precondition for employment or continued employment). But access in response to a demand by a third party may be required where the request is founded on national or Community law (an example would be certificates of marital status and the like, which might be requested in order to establish social security entitlements).

Article 13(3), corresponding to the initial Article 14(5), gives the data subject the right of rectification, erasure or suppression of data if they have been processed in violation of the Directive. Minor changes have been made in order to render the amended text more precise, as Parliament had requested (amendment No 49).

Amendment No 49 has been accepted in part. "Data which have been wholly or partially omitted" are here called "incomplete data", and are included. But the amended text retains the terms "as the case may be" and "blocking" or "suppression", which are surely useful.

For the sake of greater clarity the amended proposal uses the word "suppression" rather than the initial proposal's word "blocking". The concept is intended to cater for cases of data collected, stored, processed or used in violation of the rules in the Directive: the controller may continue to store them, but is prohibited from processing or using them, and in particular from disclosing them to third parties. The suppressed data have to be marked in the file in order to inform users of the file of the suppression.

The words "as the case may be" leave the precise determination of the data subject's entitlement to erasure, suppression or rectification in the various situations in which personal data may be processed and used in violation of the Directive to the data protection legislation of the Member States.

Article 13(4) corresponds to the initial Article 14(7). This paragraph makes provision for the data subject's interest in seeing third parties to whom inaccurate or incomplete data have been disclosed notified of the rectification, erasure or suppression so that they too can rectify, erase or suppress the data.

Article 13(5) has been added as an additional safeguard where decisions are taken by automatic means and produce results contrary to the data subject's interests. In such a case the data subject has the right to be informed of the reasoning used in the processing operation.

Article 14

Exceptions to the right of access

This corresponds to the initial Article 15. It authorizes the Member States to restrict the data subject's right of access to safeguard an overriding public interest or an interest of another person where that is equivalent to the data subject's right of privacy.

It is left to the Member States to determine whether and to what extent they want to include restrictions based on Article 14 in their domestic data protection legislation, unless they are obliged to do so under Community law (e.g. under the rules on banking supervision or money laundering). But the restrictions which the provision permits are limited to those necessary to safeguard fundamental values in a democratic society, and they must be adopted by legislation.

Parliament's amendment No 54 has been accepted. The amended Article 14 is not confined to processing carried out by the public sector, but extends to private sector processing too.

The list of the considerations justifying the restriction of access under Article 14 which is set out in paragraph 1 is exhaustive.

The term "national security" is to be interpreted as meaning the protection of national sovereignty against both internal and external threat.

"Criminal proceedings" covers the prosecution of crimes which have already been committed, whereas the concept of "public safety" encompasses all the policing functions of public authority, including crime prevention. The phrase "substantial economic and financial interests of the Member State or of the European Communities" refers to all economic policy measures and measures to finance the policies of a Member State or the Community, such as exchange controls, foreign trade controls, and tax collection. But only a substantial interest of this kind would justify a restriction of the right of access.

Lastly, other people's interests, including, where appropriate, those of the controller himself, and other people's rights and freedoms are to be considered valid grounds for restricting the right of access, provided they are equivalent to the data subject's right of access. These would include the trade secrets of others; the rules of confidentiality under which lawyers and medical practitioners operate; a person's right to prepare his or her own defence in court proceedings; and the protection of human rights. The supervisory authority ought to be obliged to place restrictions on data subjects' right of access to data relating to them held by human rights organizations where unlimited access might endanger other individuals (such as the sources of information which was provided in confidence) or the overriding interests of such organizations.

If a data subject is denied access to data relating to him contained in a file because an interest within the scope of Article 14(1) is invoked, the data protection authority must, at his request, carry out the necessary inspections and checks on the file in which the data are stored; this requirement was in the original proposal (Article 15(2)), and is now in Article 14(2). The object of the inspections and checks is to establish the lawfulness of any processing in the light of the Directive. When carrying them out, the authority must avoid harming the interests the safeguarding of which is provided for in paragraph 1.

Article 14(3), which corresponds to the original Article 15(3), empowers the Member States to place limits on the right of access to data which are compiled only temporarily, for the purpose of extracting statistical information; such operations represent only a minor threat to data subjects.

SECTION VI

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 15

Objection on legitimate grounds

Article 15(1), which corresponds to Article 14(1) in the original proposal, gives the data subject the right to object on legitimate grounds to the processing of data relating to him. "Legitimate grounds" of the kind referred to would include the absence of any legal justification for a particular processing operation, for example because the grounds for legitimate processing which are laid down in Chapter II of the Directive are not met. On the other hand a data subject would not have legitimate grounds for objecting to a legitimate processing operation which is necessary to the performance of a contract between himself and the controller.

Paragraph 2 reproduces Article 9(3) of the original proposal. Where there is an objection in accordance with paragraph 1, the controller is required to cease processing.

Paragraph 3 develops what was Article 14(6) in the initial proposal. Its aim is to clarify the obligation of the controller with regard to data subjects when he is authorized under other provisions of the Directive to disclose data to third parties for the purposes of marketing by direct mail. These obligations are to apply regardless of whether this is commercial marketing or canvassing by a charitable organization or a political party. The controller must satisfy himself that the opportunity to have data erased without cost has been expressly offered to data subjects before the data are disclosed. The same obligation is to apply where data are not disclosed but are used for the same purposes by a controller for the account of a third party. The controller may satisfy his obligations in the course of his regular correspondence with data subjects, without necessarily entering into specific correspondence.

The paragraph relates only to written mail. Measures to protect persons against unwanted approaches made through telecommunications channels are provided for in the amended proposal for a Directive in order to protect individuals in the context of telecommunications networks.

Article 16

Automated individual decisions

The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities. Article 16(1) therefore lays down the principle that a person is not obliged to accept a decision of a public administration or of a private party which adversely affects him if it is based solely on automatic processing defining a personality profile.

The version in the initial proposal has been rewritten in order more closely to define the limited cases in which these provisions are to apply.

Three conditions must be satisfied:

(i) The person must be subject to an adverse decision. The decision must be one which can be invoked against him, one which has consequences for him; thus the simple fact of sending a commercial brochure to a list of persons selected by computer is not a decision adversely affecting them for these purposes.

(ii) The decision must be taken solely by automatic processing: what is prohibited is the strict application by the user of the results produced by the system. Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgment must have its place.

It would be contrary to this principle, for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality.

(iii) The processing must apply variables which determine a standard profile (considered good or bad) to the data concerning the data subject; this excludes all cases where the system does not define a personality profile: for example, the fact that a person is unable to obtain the sum of money he wants from an automatic cash dispenser because he has exceeded his credit limit would not fall inside this definition.

A new paragraph 2 is added under which the share of human judgment required must be in proportion to the danger to the individual which would be represented by a decision which has been drawn up entirely by computer and which applies a personality profile to him.

One of Parliament's amendments (No 46) proposed that such a decision should be allowed if the person consented, or where there was a contract or a relationship of confidence approaching the state of a contract.

The amended proposal does not accept the criteria suggested; if the two sides are not on equal terms (which is the case with a job-seeker, for example) neither consent nor the hope of a contract provide a sufficient safeguard.

Under paragraph 2 a data subject may be required to accept a decision of the kind referred to in paragraph 1 if the decision is taken under a contract between the data subject and the controller, or in the course of the conclusion of such a contract, on condition that the data subject's request is met, or that there are appropriate measures to safeguard his legitimate interests (which the Member States are free to clarify). Such a safeguard might be provided by law, by the notification procedures applied, or by internal measures taken by the controller's organization.

Thus the use of scoring techniques with a view to the lending of money to an individual is possible, if positive decisions to lend are based solely on an automatic assessment of the risks; but where the score is negative the legitimate interests of the data subject must be safeguarded, for example by deferring a final answer until the organization has been able to carry out a "flesh-and-blood" study of the case.

SECTION VII

SECURITY OF PROCESSING

Article 17

This Article corresponds to Article 18 of the initial proposal.

The potential danger to the data subject's right of privacy does not emanate entirely from the controller, who collects, stores, processes and discloses the individual's data for his own purposes.

The right of privacy is also jeopardized if the data subject's data are misused by third parties who have gained unauthorized access to it.

Article 17 requires the Member States to oblige the controller to take appropriate technical and organizational measures to protect data against the danger of unauthorized intrusion by third parties, accidental or unlawful destruction, accidental loss, unauthorized alteration or any other unauthorized form of processing.

Parliament's amendment No 67 has been accepted in part. The initial proposal's "automated files" has been replaced by "the automatic processing of data". The reference to "the cost of taking the measures" has been deleted. "Controller" is the term used throughout the amended text.

Some minor changes have been made for reasons of clarity. In paragraph 1, "unauthorized destruction" has been replaced by "unlawful destruction" and "unauthorized access" has been replaced by "unauthorized disclosure". In paragraph 2 "adequate security" has been replaced by "an appropriate level of security". In paragraph 3 "on-line consultation" has been replaced by "an opportunity ... for remote access". Paragraph 4 now specifies that the security obligations also apply to persons who share responsibility for carrying out the processing, and in particular the processor.

There are two amendments of some substance. Where an opportunity is provided for remote access, paragraph 3 now specifies that hardware and software are to be utilized in such a way that access remains within the limits of the lawfulness of the processing (and not the limits of the authorization granted by the controller, which certainly would not exceed the limits of lawful processing, and is thus irrelevant for data protection purposes).

Paragraph 5 makes an exception to the obligation not to disclose data to third parties without the controller's agreement: this may be done where it is required under national or Community law (in criminal investigations, for example).

SECTION VIII

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

Article 18 reproduces Articles 7 and 11 of the initial proposal, which dealt with the notification to the supervisory authority of files created in the public and private sectors. These provisions have now been merged, as Parliament suggested in its opinion. The presentation has the advantage of showing that the approach to notification is the same in whichever sector the data are processed.

But the scope and content of the original provisions have been changed, in order to reflect Parliament's opinion and to ensure consistency in the amended proposal. Under Parliament's amendments (Nos 39, 40, 41, 118 and 199) the rules on notification are expanded in several articles. In the initial proposal notification was intended to ensure that processing operations were a matter of record; it is now to serve as the basis for selective monitoring of the legitimacy of processing operations by the supervisory authority. Depending on the degree of danger they present, monitoring of processing operations will be carried out ex post, as a general rule, or in advance, in a limited number of cases.

1. Article 18(1) amends the obligation to notify laid down in the initial proposal as follows:

   (a) For the sake of consistency in the approach taken by the amended proposal, notification would now relate to "processing" rather than to a "file". This means that supervision will concentrate more on the use made of data, and the operations carried out on data for particular purposes (the nature of the operations, combinations, disclosures to third parties, the nature of the data collected, recorded, etc.), and less on the specific technical organization of the data in the file, which may be of no great significance for the protection of individuals once data are computerized.

   (b) The fact that data might be communicated, which in the initial proposal was a criterion for the presence of this obligation, has been omitted from the amended version in view of the criticisms put forward: it was argued that it was not a suitable test, as some cases of disclosure to third parties do not infringe the rights of individuals; and there was also the danger which might be presented by purely internal processing, aimed at selecting populations. It was considered preferable to extend the obligation to all processing of personal data before the processing takes place. This approach should encourage controllers to decide on the measures necessary to meet their obligations before they commence processing. But for a proper idea of the practical scope of this amendment account has to be taken of Article 19, on simplification of and exemption from the obligation to notify.

   (c) To ensure that monitoring can take account of the often varied totality of processing operations carried out by a controller, and to avoid inviting an excessive number of notifications, it is proposed that a single notification could cover a set of processing operations, whether or not repetitive, intended to serve a single purpose or several purposes which are related between themselves from the point of view of the controller and of the data subject. By way of example, a single notification would be required for all the processing operations concerning the management of loans given by a credit institutions: this might include registering the application, investigating it, approving it, recovering debts due and keeping track of legal proceedings.

   (d) So that administration need not become too burdensome, it is proposed that the obligation to notify would apply only to processing which is wholly or partly automatic, while leaving Member States free to extend this obligation to manual files under Article 21.

2. Article 18(2) gives further details of the content of the notification.

   (a) The clause referring to the category or categories of data subject has been added (examples might be the customers of the firm, the staff of the firm, recipients of this or that social benefit, etc.).

(b) Information regarding the third parties to whom data may be disclosed may take the form of a reference to categories of third party (Parliament's amendment No 39).

(c) For the description of the data to be processed, it will now be sufficient to list the categories of data, since too great a measure of technical detail will not significantly help an understanding of the process involved.

(d) The reference to the existence of transfers of data to non-Community countries has been added in order to facilitate the application of the special rules which are to govern them, and to ensure that their specific context is taken into account.

(e) The description of the security measures which was included in the initial proposal is retained here, given the importance of being able to monitor such measures, particularly in view of the development of remote processing using telecommunications networks.

3. Article 18(3) concerns the notification of changes in the processing being carried out. The obligation to notify changes affecting the information in the earlier notification is retained from the initial proposal, so as to ensure that the list of processing operations which is accessible to the public is kept up to date, and that monitoring can continue, which is particularly important where the purposes of the processing are changed or where fresh groups of third parties may be given the data concerned.

4. Article 18(4) and (5) reflect Parliament's opinion (amendments Nos 40, 41, 118 and 199) that certain forms of processing may involve a special danger to the rights and freedoms of data subjects and should therefore be subject to a report or authorization from the supervisory authority before they are carried out.

While fully acknowledging the variety of machinery which may be established in the various Member States, the Commission feels that Article 18(4) should require Member States to have such processing examined by the supervisory authority before it is carried out. Rather than a non-binding examination Member States are free to require authorization by legislation or by the supervisory authority.

The "specific risks" referred to might have to do with the nature of the data to be processed, for example where the data is within the scope of Article 8; the scope of the processing, which might concern the whole population of a country; or the purpose in view, which might be to exclude data subjects from an entitlement, a benefit or a contract (the case of a black list or an operation aimed at informing third parties on the solvency of individuals).

Article 18(4) contains a clause intended to limit the time within which the supervisory authority must examine a case; this has been done in the controller's interest. The approach proposed in this Article should not prevent Member States from taking measures to simplify the obligation to notify, or to grant exemptions from it, as provided in Article 19, on the basis of the experience they acquire.

5. For the sake of completeness it should also be pointed out that if a wholly or partly automatic processing operation is not covered by the simplification and exemption procedures provided for in Article 19, nor subject to prior examination, but is merely notified to the supervisory authority under Article 18, it will as a rule be subject only to ex post checking by the supervisory authority, as will the processing operations referred to in Article 19. Obviously the supervisory authority will satisfy itself that the notification procedure followed corresponds to the nature of the processing.

6. In line with the spirit of Parliament's opinion (amendment No 39) the Community procedures laid down in Articles 30 and 34 should allow harmonization of particular points where this is needed for the proper operation of the single market, with special reference to Articles 18 and 19.

Article 19

Simplification of and exemption from the obligation to notify

Article 19 takes over and develops Parliament's amendment No 39, aimed at simplifying procedures for certain categories of processing.

Article 19(1) proposes that Member States should be required to take such measures; they would also be free to grant exemptions from the obligation to notify.

In order to develop a coherent Community policy on the protection of individuals, it is proposed that a criterion should be added, determining the field in which it is proper to simplify and exempt from notification. This refers to processing operations which are not liable adversely to affect the rights and freedoms of data subjects.

Experience shows that a great many operations in which personal data are processed in various organizations, large and small, public and private, are of this nature, and thus do not require any detailed or general notification. These may be forms of processing whose content and scope are by nature strictly defined in legal terms, or simple forms of processing whose legitimacy interest parties regularly have the opportunity to check, or forms of processing which by nature cannot adversely affect data subjects, or indeed forms of processing which are in fact of a more sensitive nature but which in the particular context do provide the necessary safeguards.

Article 19(1) corresponds to Parliament's amendment No 23, and proposes that a processing operation should qualify for simplification or exemption if its purpose is the production of correspondence or papers by word processing, the satisfaction of legal, accounting, tax or social security duties, or the consultation of documentation services accessible to the public.

Member States are to permit simplified procedures and to grant exemptions according to circumstances, in the light of their own experience and of the specific character of processing operations, old and new, in their own country. By way of example these measures might include the calculation of the wages and salaries of the staff of a public body or private firm, some kinds of processing for scientific research purposes, and certain operations concerning the medical records of patients held by a medical practitioner or the like.

Article 19(2) takes over Parliament's amendment No 39, under which simplification of the obligation to notify in the Member States had to be the subject of a legal act. It is now proposed, however, in the spirit of that amendment, that the drafting of a simplification or exemption measure must involve the independent supervisory authority. And in order to ensure that controllers are in a position to judge with safety whether any processing operations they envisage are in accordance with the simplification measure, it is proposed that the measure must describe each category of processing operation covered, specifying the purposes, the data or categories of data, the category or categories of data subject, the third parties or categories of third party to whom the data are to be disclosed, the length of time the data are to be stored, and where appropriate the conditions under which the processing is to be carried out.

Article 19(3) takes up the same amendment No 39; amendment No 39 also sought to make it clear that simplification or exemption from the obligation to notify is not to release the controller from any of the other obligations resulting from the Directive.

Article 20

Manual processing operations

Member States are left free to apply Section VIII to manual files, subject to whatever adaptation may be necessary.

Article 21

Register of notified processing operations

Article 21 corresponds to Article 7(1) of the initial proposal, under which the supervisory authority was to keep a register of the public sector files notified to it, which was to be freely available for consultation. In the spirit of Parliament's opinion (amendments No 37 and No 39), Article 21 now extends this provision to all notified processing operations, regardless of the sector to which the controller belongs.

Consultation of the register may however be restricted, as Parliament suggested, on the same grounds as are set out in Article 14(1), which deals with the restriction of the right of access to data by the data subject.

In line with Parliament's opinion (amendment No 39), Article 21 lays down the minimum content of entries in the register: they must include the information referred to in Article 18(2), with the exception of measures to ensure the security of processing, whose effectiveness would otherwise be reduced.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND PENALTIES

Article 22

Judicial remedies

Article 22 corresponds to Article 14(8) in the initial proposal. The scope of the provision has been broadened. It is now proposed that national legislation should provide data subjects with a judicial remedy which will enable them where necessary to defend not only the additional rights listed in Article 14 of the initial proposal but of all the rights given them by the Directive.

Article 23

Liability

Article 23(1), like Article 21(1) in the initial proposal, places a liability on the controller to compensate any damage caused to any person as a result of a processing operation or any act incompatible with the Directive. As Parliament requested in its opinion (amendment No 73), liability is made to depend on "unlawful" processing. The concept of a "file" is replaced by that of "processing". The change of wording means that the content of paragraph 2 in Parliament's suggested version has in fact been incorporated here. By speaking about "processing" the amended proposal now includes the actual storage of personal data as a possible source of liability, as Parliament had hoped.

But the Commission still feels that Member States should be free to exempt from liability where suitable security measures have been taken. The wording of the provision has been clarified. In view of Parliament's opinion the Commission now specifies that a controller may be exempted in whole or only in part.

Article 24

Processing by the processor

This Article corresponds to Article 22 of the original proposal. It aims to ensure that the protection of the data subject is not deleted where processing is carried out by a third party on the controller's behalf.

The Article uses the term "processor", which has been included in the list of definitions at Parliament's suggestion. In accordance with Parliament's wishes, paragraph 2 emphasizes that the processor may act only within the terms of his contract with the controller. It is proposed that an express reference should be made to the obligations imposed by the national measures taken under the Directive, which will also apply to a processor.

Article 25

Penalties

The changes made to the proposal here are intended to take account of Parliament's opinion (amendment No 77). They shift the accent to the persons who may be punishable. Penalties may in general be imposed on any person who does not comply with the national provisions adopted pursuant to the Directive, which may include, as Parliament points out in its opinion, authorities and organizations governed by public law.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 26

Principles

This Article corresponds to Article 25 in the initial proposal; it states that the transfer of personal data from a Member State to a non-member country may take place only if the non-member country ensures an adequate level of protection. Without such a provision the Community's efforts to guarantee a high level of protection for individuals could be nullified by transfers to other countries in which the protection provided is inadequate. There is also the fact that free movement of data between Member States, which the proposal seeks to establish, will mean that there will have to be common rules on transfer to non-Community countries.

In the course of consultation with interested parties it became clear that in certain cases there would have to be exceptions to this principle. The Commission has therefore reconsidered its initial proposal, in the light of Parliament's opinion. It now proposes that the ban on transfers to non-member countries which do not provide an adequate level of protection should be subject to exceptions compatible with the protection of individuals. Under the amended proposal, a transfer may be made to a country which does not ensure an adequate level of protection if the data subject has consented in order to take steps preliminary to entering into a contract, or if the transfer is necessary for the performance of a contract between the data subject and the controller. In such cases the data subject must have been informed that it is or might be proposed to transfer the data to such a country. The data subject may decide whether or not he wishes to take such a risk. These exceptions seem particularly useful in the case of data transfers linked to the transactions of banks or other credit institutions. A transfer to a non-member country which does not provide an adequate level of protection may also be justified if it is necessary on important public interest grounds or in order to protect the vital interests of the data subject. These exceptions are intended to allow international cooperation (e.g. to combat money laundering or in monitoring financial institutions) or to allow the transfer of medical information in circumstances in which the data subject is unable to express his wishes.

Paragraph 2 describes the tests to be applied to determine whether or not protection is adequate. Account is to be taken of all the circumstances surrounding a data transfer operation or set of data transfer operations, such as the nature of the data, the purpose of the processing operations, and the legislation in force in the other country. Both general and sectoral legislative provisions will have to be examined here, along with the question whether they are applied in practice, and any professional rules laid down in codes of conduct. As Parliament suggested in its opinion (see amendment No 79), the new paragraph 2 makes it clear that the adequacy of protection is to be assessed with reference to a transfer of data or a set of transfers of data.

Paragraph 3, which corresponds to Article 24(2) in the initial proposal, has been amended in line with Parliament's opinion (amendment No 79), which emphasizes that Member States are to assess the adequacy of protection and to decide whether or not to ban data transfers accordingly. They are to inform the Commission of such cases of prohibition.

As Parliament requested (amendment No 80), the Commission is to consult the Working Party referred to in Article 32 before entering into negotiations with a non-Community country; this is stipulated in paragraph 4, which corresponds to the old Article 24(3).

Article 27

Particular measures

Article 27 reflects the intention of Article 25 of the initial proposal, with some modifications. Under the new version a Member State may authorize a transfer or category of transfers of personal data to a non-member country which does not ensure an adequate level of protection if the controller adduces sufficient justification guaranteeing the effective exercise of data subjects' rights, and if the other Member States or the Commission do not object to the measure envisaged in accordance with a procedure which the Article lays down. If an objection is made the Commission is to take appropriate measures, and may in particular decide to prohibit the transfer, to make it subject to additional conditions, or to enter into negotiations with the controller for whom the transfers are to be made in order to arrive at solutions for the whole Community.

CHAPTER V

CODES OF CONDUCT

Codes of conduct - the term generally used in other fields is the one employed in the amended proposal - were covered by Article 20 in the initial proposal. That provision aimed to encourage the drawing up of Community codes only. The amended proposal contains two Articles, one dealing with national codes and the other with Community codes.

Article 28

National codes

In the light of the experience gained by certain Member States, the Commission has decided to include in its amended proposal a provision aimed at encouraging the drawing up of codes of conduct at national level. Such codes can make for better acceptance of the legislation, since those operating in the field can participate directly in implementing the legislation. They also help to avoid over-detailed legislation, always provided the solutions they contain are satisfactory. Codes of conduct vary widely in terms of their substance, the trade associations which have drawn them up, and so on. But they all have the following features:

- they are drawn up voluntarily by a profession or trade, although they may be encouraged by the authorities;

- they apply or fill out the legislation applicable, but they must remain within it;

- they are not binding on third parties, or on the courts, which may always give priority to their own interpretation of the legislation.

Of course it may happen that the public authorities, and the legislature in particular, themselves adopt a code drawn up by the trade, and give it binding legislative force; this has happened in certain Member States.

To give such codes some authority, without changing their essential characteristics, the Commission proposes that they should be submitted to the competent national authority for its opinion; in doing this the Commission is basing itself on the approach taken by Parliament in the case of Community codes (amendment No 72).

It is therefore proposed that the supervisory authority should be asked to check that codes are well thought out and that the trade associations which drew them up are representative, and to ensure that codes are publicized, to take the views of interested parties or their representatives, and to deliver an opinion to be published alongside the code.

Article 29

Community codes

The amended proposal follows the lines of Parliament's opinion (amendment No 72) and the provisions of Article 28, the powers given to the national supervisory authority in the case of national codes being given here to the Community working party on data protection. It will be for the Commission to decide whether or not to publish codes together with the working party's opinion for information purposes in the Official Journal.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY

Article 30

Supervisory authority

This Article corresponds to Article 26 in the initial proposal; it provides for the setting up of a supervisory authority, the essential feature of which would be its independence. The Commission has accepted Parliament's opinion (amendments Nos 84, 85, 86 and 87), and incorporated Parliament's amendments into its own amended proposal.

(a) Designation of supervisory authorities: Paragraph 1 makes it clear that Member States are free to designate several independent supervisory authorities. This seems indispensable for Member States with a federal structure, and for Germany in particular.

(b) Powers of supervisory authorities: In addition to the powers given to supervisory authorities by the provisions already discussed, particularly in connection with notifications, it is proposed that supervisory authorities should have powers of investigation and intervention in their dealings with controllers, under judicial control.

The supervisory authority's powers of investigation are intended to enable it to collect from controllers the information it needs to perform its duties. The authority would have access to the data being processed. In order to preserve the rights of those subject to supervision by the authority, obviously, these powers must be exercised in strict observance of the confidentiality of the relevant data under national law. A provision to this effect is inserted in paragraph 6.

To enable the supervisory authority to carry out its duties it must also have effective powers of intervention, such as those enumerated by Parliament in its opinion, and repeated in the amended proposal: power to order suppression, erasure of data, a ban on the processing operation, etc. Parliament referred to these measures as "sanctions", but it does not appear necessary that the Directive should define their legal nature.

Lastly, it is proposed that the supervisory authority should have power to bring an action before the courts where it finds that the national provisions implementing the Directive have been infringed. The existing systems of national legislation generally confer such a right. The right follows logically from the power of investigation, as it is only reasonable that an authority whose duty is to protect individuals should not set the machinery of justice in motion where it finds an infringement of their right to protection, and also from the right of any person to lodge a complaint with the supervisory authority: the consequence of such a complaint should indeed be a reference to the courts.

(c) Annual reports: It is very important that the supervisory authority should be able to present a report on its activities at periodic intervals, pointing out any difficulties it has met in applying the legislation, and indicating the new approach to be taken.

Article 31

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

This Article corresponds to Article 27 in the initial proposal, and sets up a committee of the advisory type.

(a) Name of the working party

It is proposed that the title of the working party be aligned on the wording in Article 1(1).

(b) Membership and chair

The amendments requested by Parliament (amendments No 88 and No 128) are concerned mainly with the membership and chairmanship of the Working Party. In order to guarantee the working party's independence, a point it emphasized in the explanatory memorandum to the initial proposal, the Commission has accepted the suggestions in Parliament's opinion regarding the chairmanship of the working party, but not those regarding its membership.

(i) Chairmanship: the Commission is proposing that the working party should elect a chairman for a renewable term of two years. This term seems sufficiently long to ensure a measure of stability.

(ii) Membership: the Commission is maintaining its initial proposal that membership should be restricted to representatives of the national supervisory authorities already referred to. If some Member States make use of their freedom to designate more than one supervisory authority, it is proposed for the sake of fairness that those Member States should be represented by a joint representation on the working party. Otherwise the fact that a Member State had taken advantage of the freedom left to it by the preceding Articles might produce an unbalanced representation on the Working Party.

The Commission is asking that it should be represented on this working party, and hopes that its own departments can provide the secretarial services.

Article 32

Tasks of the Working Party

This Article defines the tasks of the Working Party. The Working Party would continue to be an advisory body, as provided in the initial proposal. It would advise the Commission, particularly when it was proposed that the Commission should exercise its rule-making powers or put forward new proposals. It would help to ensure that provisions adopted pursuant to the Directive were applied in a uniform fashion, and also with the development of a common policy on cross-border flows of data between the Community and non-Community countries. The Commission would submit to the Working Party any measure proposed in these fields with a view to obtaining its opinion.

The Working Party would act through opinions and recommendations submitted to the Commission and possibly to the Advisory Committee. Here the proposal accepts Parliament's opinion in part (amendments Nos 90, 91 and 92).

The Commission is to inform the Working Party of the action it has taken in response to its opinions and recommendations, in a public report which is to be transmitted to Parliament and to the Council.

The Commission shares Parliament's concern, expressed in amendment No 89, that the secretariat of the Working Party should be allocated the necessary funds to enable it to carry out the tasks given to it by the Directive. In the budgetary procedure and elsewhere the Commission will seek to ensure that the Working Party does have sufficient funding. But is does not appear advisable to include a provision to this effect in the amended proposal.

CHAPTER VII

RULE MAKING POWERS OF THE COMMISSION

Articles 33 and 34

Exercise of rule making powers and Advisory Committee

The Community maintains its initial proposal. Technical measures will be needed to apply the Directive given the breadth and the highly technical nature of the field of personal data processing.

FINAL PROVISIONS

Articles 35, 36 and 37

Article 35(2) proposes a transitional measure in line with what Parliament suggested for notification (amendment No 37), namely that the provisions adopted under the Directive should enter into force more slowly in respect of processing operations which began before the date on which those provisions enter into force. A three-year period seems sufficient.

As Parliament hoped (amendment No 95) it is proposed in Article 36 that the regular report on the implementation of the Directive which the Commission is to send the Council and Parliament should also be published.

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,

In cooperation with the European Parliament,

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

AMENDED PROPOSAL FOR A COUNCIL DIRECTIVE ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH 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) OJ No C 277, 5.11.1990, p. 3; OJ No C ...

(2) OJ No C ...; OJ No C ...

(3) OJ No C 159, 17.6.1991, p. 38.

(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;

(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;

(7)

	(2) Whereas data-processing systems are designed to serve society; whereas they must respect the fundamental freedoms and rights of individuals, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;
(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 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 from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(3) Whereas the internal market comprises an area without frontiers; whereas, for that reason, the national authorities in the various Member Sttes are increasingly being called upon, by virtue of the operation of Community lax, 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;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 8a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon, by virtue 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 within the context of the area without internal frontiers as constituted by the internal market;

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

(5) Whereas the difference in levels of protection of privacy in relation to the processing of personal dat 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 lax; 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, furthermore, 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;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard 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 floxs 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;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all the Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 8a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(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;

(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;

(9) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European 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;

(10) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are 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;

(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;

(11) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas processing carried out by a Member State's own authorities, organizations or other bodies in the course of activities 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 out in national laws; whereas processing carried out by a natural person for purely private purposes in connection, for example, with correspondence or the maintenance of lists of addresses 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 separte data file and transfer to a non-member country must not be a bar to such protection;

(12) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out by a person who is established in a Member State should be governed by the law of that State; whereas, the fact that processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas, in that case, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(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 Member States may more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas, however, more precise rules of this kind cannot serve as a basis for supervision by a Member State other than the Member State of residence of the person responsible for the processing, since the obligation on the part of the latter to ensure, in accordance with this Directive, the protection of rights and freedoms with regard to the processing of personal data is sufficient, under Community law, to permit the free flow of data;

(14) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises or bodies carrying out processing, in particular regarding quality, technical security, notification to the supervisory authority, and the circumstances under which processing is admissible, one such possible circumstance being that the data subject has consented, and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of

processing, to be informed that processing is taking place, to consult the data, to demand corrections and even to object to processing;

(15) Whereas any processing of personal data must be lawful and fair to the person concerned; whereas, in particular, the data must be relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and lawful;

(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;

(16) Whereas, in order to be lawful, the processing of personal data must be carried out with the consent of the data subject or with a view to the conclusion or performance of a contract, binding on the data subject, or be required by Community law, by national law, by the general interest or by the interest of an individual, provided that the data subject has no legitimate grounds for objection; whereas, in particular, in order to maintain a balance between the interests involved, while guaranteeing effective competition, Member States remain free to determine the circumstances in which personal

data may be disclosed to a third party for mailing purposes or research being carried out by an organization or other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the disclosure of data regarding him, at no cost and without having to state his reasons;

(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 data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his written consent; whereas, however, processing of these data must be permitted if it is carried out by an association the purpose of which is to help safeguard the exercise of those freedoms; whereas, on grounds of important public interest, notably in relation to the medical profession, exemptions may be granted by law or by decision of the supervisory authority laying down the limits and suitable safeguards for the processing of these types of data;

(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;

(18) Whereas the processing of personal data for purposes of journalism should qualify for exemption from the requirements of this Directive wherever this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the protection of Human Rights and Fundamental Freedoms;

(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;

(19) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and must be given accurate and full information where data are collected from him, and not later than the time when the data are first disclosed to a third party if the data subject was not informed at the time the data were collected;

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

(20) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify the accuracy of the data and the lawfulness of the processing; whereas, therefore, any person should be entitled to object to the processing of the data on legitimate grounds;

(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;

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;

(21) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical measures be taken, both at the time of the design of the techniques of processing and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing;

(22) Whereas the notification procedures are designed to ensure disclosure of the purposes and main features of any processing operation, for the purpose of verification that the operation is in accordance with the national measures taken under this Directive; whereas, in order to avoid unsuitable administrative formalities, exemption from the obligation to notify and simplification of the notification required must be provided for by Member States in cases where processing does not adversely affect the rights and freedoms of data subjects provided that it is in accordance with a measure taken by a Member State and specifying its limits;

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

(23) Whereas ex post facto verification by the competent authorities must, in general, be considered a sufficient measure; whereas, however, Member States must provide for checking by the supervisory authority prior to any processing which poses a particular threat to the rights and freedoms of data subjects by virtue of its nature, scope or purpose, such as processing which has as its object the exclusion of data subjects from a right, a benefit or a contract; whereas Member States should be entitled to replace such prior checking by means of a legislative measure or a decision of the supervisory authority authorizing the processing operation and specifying suitable safeguards;

(24) Whereas, if the person carrying out processing fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the person responsible for the processing, who may be exempted from liability only if he proves that he has taken suitable security measures;

whereas dissuasive penalties must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(21) Whereas 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;

(25) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(26) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited; whereas provision should be made for exemptions in certain circumstances where the data subject has given his consent or has been informed or where protection of the public interest so requires; whereas particular measures may be taken to rectify the lack of protection in a third country in cases where the person responsible for the processing offers appropriate assurances; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(27) Whereas Member States may also provide for the use of codes of conduct drawn up by the business circles concerned and approved by the supervisory authority, with a view to adapting the national measures taken under this Directive to the specific characteristics of processing in certain sectors;

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;

(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;

(28) Whereas Member States must encourage the business circles concerned to draw up Community codes of conduct so as to facilitate the application of this Directive; whereas the Commission will support such initiatives and will take them into account when it considers the appropriateness of additional specific measures in respect of certain sectors;

(29) Whereas the establishment in each Member State of an independent supervisory authority is an essential component of the protection of individuals with regard to the processing of personal data; whereas such an authority must have the necessary means to perform its duties, including powers of investigation or intervention and powers in connection with notification procedures; whereas such authority must help to ensure transparency of processing in the Member State within whose jurisdiction it falls; whereas the authorities in the different Member States will need to assist one another in performing their duties;

(30) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing 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, in particular, 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 aof an Advisory Committee in accordance with the procedures laid down in Council Decision 87/373/EEC (4);

(31) Whereas the adoption of additional measures for applying the principles set out 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 (4);

(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,

(32) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(4) OJ No L 197, 18.7.1987, p. 33.

(4) OJ No L 197, 18.7.1987, p. 33.

(33) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules gradually to all processing operations already under way;

(34) Whereas this Directive does not stand in the way of a Member State's regulating market research activities aimed at consumers residing in its territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data,

CHAPTER 1

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.

CHAPTER 1

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right of privacy.

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

Article 2 **Definitions**	Article 2 **Definitions**
For the purposes of this Directive:	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 similar identifying particular;	(a) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; Data presented in statistical form, which is of such a type that the persons concerned can no longer be reasonably identified, are not considered as personal data.

(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;

(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;

(b) "processing of personal data" ("processing") means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(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;

(c) "personal data file" ("file") means any structured set of personal data, whether centralized or geographically dispersed, which is accessible according to specific criteria and whose object or effect is to facilitate the use or alignment of data relating to the data subject or subjects;

(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;

(d) "controller" means any natural or legal person, public authority, agency or other body who processes personal data or causes it to be processed and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them;

(e) "processor" means any natural or legal person who processes personal data on behalf of the controller;

(f) "third party" means any natural or legal person other than the data subject, the controller and any person authorized to process the data under the controller's direct authority or on his behalf;

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;

(g) "the data subject's consent" means any express indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed, on condition he has available information about the purposes of the processing, the data or categories of data concerned, the recipient of the personal data, and the name and address of the controller and of his representative if any;

The data subject's consent must be freely given and specific, and may be withdrawn by the data subject at any time, but without retrospective effect.

(f) "supervisory authority" means the independant 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 wherre 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 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which forms part of a file or is intended to form part of a file.

2. This Directive shall not apply:

- to the processing of data in the course of an activity which falls outside the scope of Community law;

- to the processing of personal data by a natural person in the course of a purely private and personal activity.

Article 4 **Law applicable**	**Article 4** **National law applicable**
1. Each Member State shall apply this Directive to:	1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:
(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.	(a) of which the controller is established in its territory or is within its jurisdiction;
	(b) of which the controller is not established in the territory of the Community, where for the purpose of processing personal data he makes use of means, whether or not automatic, which are located in the territory of that Member State.

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.

2. In the circumstances referred to in paragraph 1(b) the controller must designate a representative established in the territory of that Member State, who shall be subrogated to the controller's rights and obligations.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall provide that the processing of personal data is lawful only if carried out in accordance with this Chapter.

Subject to this Chapter, Member States may more precisely determine the circumstances in which the processing of personal data is lawful.

CHAPTER V

DATA QUALITY

Article 16

Principles

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

(a) collected and processed fairly and lawfully;

(b) stored for specified, explicit and lawful purposes and used in a way compatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, if necessary, kept up to date; inaccurate or incomplete data shall be erased or rectified;

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

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

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate 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 processed;

(d) accurate and, where necessary, kept up to date; every step must be taken to ensure that data which are inaccurate or incomplete having regard to the purposes for which they were collected are 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.	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes in view; Member States may lay down appropriate safeguards for personal data stored for historical, statistical or scientific use.
2. It shall be for the controller of the file to ensure that paragraph 1 is complied with.	2. It shall be for the controller to ensure that paragraph 1 is complied with.
CHAPTER II	SECTION II
LAWFULNESS OF PROCESSING IN THE PUBLIC SECTOR	**PRINCIPLES RELATING TO THE GROUNDS FOR PROCESSING DATA**
Article 5 Principles	Article 7
1. Subject to Article 6, the Member States shall, with respect to files in the public sector, provide in their law that:	Member States shall provide that personal data may be processed only if:

(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 limites 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.

(a) the data subject has consented;

(b) processing is necessary for the performance of a contract with the data subject, or in order to take steps at the request of the data subject preliminary to entering into a contract;

(c) processing is necessary in order to comply with an obligation imposed by national law or by Community law;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task in the public interest or carried out in the exercise of public authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary in pursuit of the general interest or of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject.

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 specifiy 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.

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.

CHAPTER V

DATA QUALITY

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.

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade-union membership, and of data concerning health or sexual life.

2. Member States shall provide that data referred to in paragraph 1 may be processed where:

(a) the data subject has given his written consent to the processing of that data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be waived by the data subject giving his consent;

(b) processing is carried out by a foundation or non-profit-making association of a political, philosophical, religious or trade union character in the course of its legitimate activities and on condition that the processing relates solely to members of the foundation or association and to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to third parties without the data subject's consent; or

(c) the processing is performed in circumstances where there is manifestly no infringement of privacy or fundamental freedoms.

The processing of data referred to at point (b) shall not be subject to the obligation to notify imposed in Section VIII of this Chapter.

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. Member States may, on grounds of important public interest, lay down exemptions from paragraph 1 by national legislative provision or by decision of the supervisory authority, stating the types of data which may be processed, the persons to whom such data may be disclosed and the persons who may be controllers, and specifying suitable safeguards.

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

4. Data concerning criminal convictions may be held only by judicial and law-enforcement authorities and by the persons directly concerned with those convictions or by their representatives; Member States may, however, lay down exemptions by means of a legislative provision which shall specify suitable safeguards.

5. Member States shall determine the conditions under which a national identification number or other identifier of general application may be used.

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 9

Processing of personal data and freedom of expression

With a view to reconciling the right to privacy with the rules governing freedom of expression, Member States shall prescribe exemptions from this Directive in respect of the processing of personal data solely for journalistic purposes by the press, the audio-visual media and journalists.

CHAPTER IV

RIGHTS OF DATA SUBJECTS

Article 14

Additional rights of data subjects

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

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.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

The existence of a processing operation

1. Member States shall ensure that any person is entitled, on request, to know of the existence of a processing operation, its purposes, the categories of data concerned, any third parties or categories of third party to whom the data are to be disclosed, and the name and address of the controller and of his representative, if any.

2. Member States may lay down exemptions from paragraph 1 in the circumstances referred to in Article 14(1).

Article 13 **Provision of information at the time of collection**	Article 11 **Collection of data from the data subject**
1. The Member States shall guarantee individuals from whom personal data are collected the right to be informed at least about:	1. Member States shall provide that the controller must ensure that a data subject from whom data are collected be informed at least of the following:
(a) the purposes of the file for which the information is intended;	(a) the purposes of the processing for which the data are intended;
(b) the obligatory or voluntary nature of their reply to the questions to which answers are sought;	(b) the obligatory or voluntary nature of any reply to the questions to which answers are sought;
(c) the consequences if they fail to reply;	(c) the consequences for him if he fails to reply;
(d) the recipients of the information;	(d) the recipients or categories of recipients of the data;
(e) the existence of the right of access to and rectification of the data relating to them; and	(e) the existence of a right of access to and rectification of the data relating to him; and

(f) the name and address of the controller of the file.

(f) the name and address of the controller and of his representative if any.

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 order.

2. Paragraph 1 shall not apply to the collection of data where to inform the data subject would hinder or prevent the exercise of or the co-operation with the supervision and verification functions of a public authority or the maintenance of public order.

CHAPTER III

LAWFULNESS OF PROCESSING IN THE PRIVATE SECTOR

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.

Article 12

Disclosure to a third party

1. Member States shall provide that in the cases referred to in Article 7(b), (c), (e) and (f) the controller must satisfy himself that at the appropriate time, and no later than the time when the data are first disclosed to a third party, the data subject is informed of this disclosure and of the following information at least:

(a) the name and address of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) the categories of data concerned;
(d) the recipients or categories of recipients; and
(e) the existence of rights of access, rectification and objection.

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 olbigation 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.

2. Paragraph 1 shall not apply where:
- the data subject has already been informed that the data are to be or may be disclosed to a third party;
- disclosure to a third party is required by a legal provision which lays down an exemption from the obligation to inform; or
- the data are disclosed to a third party for one of the reasons listed in Article 14(1).

Article 10

Special exception 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 intrest of a third party, the Member States may provide in their law that the supervisory authority may authorize a derogation.

3. Where the provision of information to the data subject proves impossible or involves a disproportionate effort, or runs counter to the overriding legitimate interests of the controller or similar interests of a third party, Member States may empower the supervisory authority to authorize an exemption, laying down any suitable safeguards.

CHAPTER IV

RIGHTS OF DATA SUBJECTS

Article 14

Additional rights of data subjects

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

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 13

Right of access

Member States shall grant all data subjects the following rights:

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

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

5. To obtain, as the case may be, rectification, erasure or blocking of such data if they have been processed in violation of the provisions of this Directive.

1. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the existence of personal data relating to him, communication to him of such data in an intelligible form, an indication of their source, and general information on their use.

Member States may provide that the right of access to medical data may be exercised only through a medical practitioner;

2. to refuse any demand by a third party that he should exercise his right of access in order to communicate the data in question to that third party or to another party, unless the third party's request is founded on national or Community law;

3. to obtain, as the case may be, the rectification of inaccurate or incomplete data or the erasure or blocking of such data if they have been processed in breach of this Directive;

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.

4. where point 3 applies, to be notified of the rectification, erasure or blocking to any third party to whom the data have been disclosed;

5. to be informed of the reasoning applied in any automatic processing operations the outcome of which is invoked against him.

Article 15

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

Article 14

Exceptions to the right of access

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

1. Unless obliged to do so by a provision of Community law, Member States may restrict the exercise of the rights provided for in Article 10(1) and in point 1 of Article 13 where such restriction is necessary to safeguard:

(a) national security;

(a) national security;

(b) defence;

(b) defence;

(c) criminal proceedings;

(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.

(d) public safety;

(e) a duly established paramount economic and financial interest of a Member State or of the Community;

(f) a monitoring or inspection function performed by a public authority or an activity undertaken to assist the performance of such a function;

(g) an equivalent right of another person and the rights and freedoms of others.

2. In the circumstances described in paragraph 1, the supervisory authority shall be empowered to carry out the necessary checks, at the data subject's request, so as to verify the lawfulness of the processing within the meaning of this Directive, respecting the interests to be protected in accordance with paragraph 1.

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.

3. Member States may limit the right of access of the person concerned to data temporarily kept in personal form and which is intended to serve statistical ends of such a type that the persons concerned can no longer be reasonably identified.

SECTION VI

THE DATA SUBJECT'S RIGHT TO OBJECT

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.

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.

Article 15

Objection on legitimate grounds

1. Member States shall grant the data subject the right to object at any time on legitimate grounds to the processing of data relating to him.

2. Where there is a justified objection, the controller shall cease the processing.

3. The controller must ensure that the opportunity to have data erased without cost has been expressly offered to a data subject before personal data are disclosed to third parties or used on their behalf for the purposes of marketing by mail.

Article 16

Automated individual decisions

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.

1. Member States shall grant the right to every person not to be subjected to an administrative or private decision adversely affecting him which is based solely on automatic processing defining a personality profile.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided any request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, which must include arrangements allowing him to defend his point of view; or

(b) is authorized by law which also lays down measures to safeguard the data subject's legitimate interests.

CHAPTER V

DATA QUALITY

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 acidental or unauthorized destruction or accidental loss and against unauthorized access, modification or other processing.

SECTION VII

SECURITY OF PROCESSING

Article 17

1. Member States shall provide that the controller must take appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration or disclosure or any other unauthorized form of 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.	Such measures shall ensure, in respect of the automatic processing of data, a suitable level of security having regard to the state of the art and the nature of the data to be protected, and an evaluation of the potential risks involved. To that end, the controller shall take into consideration any recommendations on data security and network interoperability made by the Commission in accordance with the procedure referred to in Article 33.
2. Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network.	2. Methods ensuring an appropriate level of security shall be chosen for the transmission of personal data within a network.
3. In the event of on-line consultation, the hardware and software shall be designed in such a way that the consultation tkaes place within the limits of the authorization granted by the controller of the file.	3. Where an opportunity is provided for remote access, the controller shall utilize the hardware and software in such a way that the access takes place within the limits of the lawfulness of the processing.

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.

4. The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who share responsibility for carrying out the processing, and, in particular, on the processor.

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.

5. Any person who, in the course of his work, has access to personal data shall not disclose it to third parties without the controller's agreement, unless he is required to do so under national or Community law.

CHAPTER II

LAWFULNESS OF PROCESSING IN THE PUBLIC SECTOR

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.

SECTION VIII

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 30 before carrying out any wholly or partly automatic processing or a set of processing operations of the same type intended to serve a single purpose or several related purposes.

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).

2. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the processing;
(c) the category or categories of data subject;
(d) a description of the data or of the categories of data to which the processing relates;
(e) the third parties or categories of third party to whom the data might be disclosed;
(f) proposed transfers of data to third countries;
(g) a description of the measures taken pursuant to Article 17 to ensure security of processing.

CHAPTER III

LAWFULNESS OF PROCESSING IN THE PRIVATE SECTOR

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.

3. Any change affecting the information referred to in paragraph 2 must be notified to the supervisory authority.

4. Before processing which poses specific risks to the rights and freedoms of individuals commences, the supervisory authority shall examine such processing within a period of 15 days commencing with the date of the notification at the end of which period the authority shall give its conclusions.

5. Member States may provide that some of the processing operations referred to in paragraph 4 shall be authorized beforehand either by law or by decision of the supervisory authority.

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.

Article 19

Simplification of and exemption from the obligation to notify

1. Member States shall provide for the taking of measures to simplify or exempt from the obligation to notify in the case of certain categories of processing operation which do not adversely affect the rights and freedoms of data subjects. Such categories of processing include the production of correspondence or papers, the satisfaction of legal, accounting, tax or social security duties or the consultation of documentation services accessible to the public.

2. Simplification or exemption measures shall be adopted either by or after consulting the supervisory authority. Such measures shall particularly specify, for each category of processing operation:

- the purposes of the processing;
- a description of the data or categories of data undergoing processing;
- the category or categories of data subject;
- the third parties or categories of third party to whom the data are to be disclosed;

- the length of time the data are to be stored;
- where appropriate, the conditions under which the processing is to be carried out.

3. Simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive.

Article 20

Manual processing operations

Member States may lay down the conditions under which Articles 18 and 19 are to apply to non-automatic processing operations involving personal data contained in files.

Article 21

Register of notified processing operations

Member States shall provide that a register of notified processing operations must be maintained by the supervisory authority. The register shall as a minimum in the cases provided for in Articles 18 and 19, contain the information listed in Article 18(2)(a) to (f). It may be inspected by any person subject to such restrictions as may be imposed by Member States on the same grounds as are set out in Article 14(1).

CHAPTER VI

PROVISIONS SPECIFICALLY RELATING TO CERTAIN SECTORS

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 IV

RIGHTS OF DATA SUBJECTS

Article 14

Additional rights of data subjects

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

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

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND PENALTIES

Article 22

Judicial remedies

Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed by 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 23
Liability

1. Member States shall provide that any person whose personal data are undergoing processing and who suffers damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. Member States may provide that the controller may be exempted, in whole or in part, from his liability for damage resulting from the loss or destruction of data or from unauthorized access if he proves that he has taken suitable steps to satisfy the requirements of Articles 17 and 24.

Article 22

Processing on behalf of the controller of the file

1. The Member States shall provide in their law that the controller of the file must, where processing is carried out on his behalf, ensure that the necessary security and organizational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.

2. Any person who collects or processes personal data on behalf of the controller of the file shall fulfil the obligations provided for in Article 16 and 18 of this Directive.

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

Article 24

Processing on behalf of the controller

1. Member States shall provide that the controller must, where processing is carried out on his behalf, ensure that the necessary security and organizational measures are taken and choose a processor who provides sufficient guarantees in that respect.

2. The processor shall carry out only such processing of personal data as is stipulated in his contract with the controller and shall take instructions only from the latter. He shall comply with the national provisions adopted pursuant to this Directive.

3. The contract shall be in writing and shall state, in particular, that personal data processed thereunder may be disclosed to a third party by the processor or his employees only with the controller's agreement.

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.

Article 25

Penalties

Each Member State shall provide for the imposition of dissuasive penalties on any person who does not comply with the national provisions adopted 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.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 26

Principles

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

Notwithstanding the first subparagraph, Member States shall provide that a transfer to a third country which does not ensure an adequate level of protection may take place on condition that:

- subject, where appropriate, to Article 8(2)(a), the data subject has consented to the proposed transfer in order to take steps preliminary to entering into a contract;
- the transfer is necessary for the performance of a contract between the data subject and the controller, on condition that the data subject has been informed of the fact that it is or might be proposed to transfer the data to a third country which does not ensure an adequate level of protection;
- the transfer is necessary on important public interest grounds; or
- the transfer is necessary in order to protect the vital interests of the data subject.

	2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular account shall be taken of the nature of the data, the purpose or purposes and duration of the proposed processing operation or operations, the legislative provisions, both general and sectoral, in force in the third country in question and the professional rules which are complied with in that country.
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. Member States shall inform the Commission of cases where they consider that a 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. 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 ensure 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.

5. The Commission may decide, in accordance with the procedure laid down in Article 34(2) 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.

6. 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 persons with regard 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 conroller of the file of sufficient proof that an adequate level of protection will be provided. The Member State may grant a derogation only after it has informed the Commission and the Member States thereof and in the absence of notice of opposition given by a Member State or the Commission within a period of 10 days.

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

Article 27

Particular measures

1. Subject to the second subparagraph of Article 26(1), a Member State may authorize a transfer or category of transfers of personal data to a third country which does not ensure an adequate level of protection where the controller adduces sufficient justification in particular in the form of appropriate contractual provisions guaranteeing, especially, the effective exercise of data subjects' rights.

2. The Member State shall inform the Commission and the other Member States in good time of its proposal to grant authorization.

3. If a Member State or the Commission objects before the authorization takes effect, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 34(2).

CHAPTER V

CODES OF CONDUCT

Article 28
National codes

1. Member States may provide that codes of conduct drawn up by trade associations may make additional provision for the special features of particular sectors, subject to the national measures taken under this Directive.

2. The draft codes shall be reviewed by the national supervisory authority, which shall ascertain whether or not they are justified and the representativeness of the organizations which prepared them. The authority shall seek the views of data subjects or their representatives.

3. Member States shall ensure the official publication of codes which have been the subject of a favourable opinion on the part of the supervisory authority.

4. Any extension or amendment of the codes shall be subject to identical procedures.

Article 29

Community codes

1. Member States and the Commission shall encourage the trade associations concerned to participate in drawing up Community codes of conduct intended to contribute to the proper application of this Directive in the light of the specific characteristics of each sector.

2. The Commission may, for the purposes of information, publish codes of conduct in the Official Journal of the European Communities, together with the opinion of the Working Party provided for in Article 31 on the content of the codes and the representativeness at Community level of the organizations which prepared them. The Working Party shall seek the views of data subjects or their representatives.

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.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 30

Supervisory authority

1. Each Member State shall designate an independent public authority to supervise the protection of personal data. The authority shall be responsible for monitoring the application of the national provisions adopted pursuant to this Directive and for performing all the functions entrusted to it by this Directive. Each Member State may designate more than one supervisory authority.

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.

2. Each supervisory authority shall have:
   - investigative powers including the right of access to data forming the subject-matter of processing operations covered by this Directive and the right to collect all the information necessary for the performance of its supervisory duties;
   - effective powers of intervention such as ordering the blocking or erasure of data, a temporary or definitive ban on processing or the destruction of data material, or warning the controller;
   - the power to bring an action before the courts where it finds that the national provisions implementing this Directive have been infringed.

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

3. Each supervisory authority shall hear complaints lodged by any person concerning the protection of persons with regard to the processing of personal data. The person concerned shall be informed of the outcome of the complaint.

4. Each supervisory authority shall produce an annual report. The report shall be made public.

5. Member States' authorities shall cooperate with one another to the extent necessary for the performance of their supervisory duties, inter alia by exchanging useful information or exercising their powers of investigation or intervention.

6. Member States shall provide that the supervisory authority, its members and its staff are to be subject to a duty of confidence.

Article 27

Working Party on the Protection of Personal Data

1. A Working Party on the Portection 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.

Article 31

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as "the Working Party", is hereby set up. The Working Party, which shall have advisory status, shall act independently. It shall be composed of representatives of the supervisory authorities provided for in Article 30 and of a representative of the Commission.

	Where a Member State designates more than one supervisory authority, those authorities shall appoint joint representatives who, within the Working Party, shall have the same rights and obligations as the other representatives of the other authorities.
	2. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.
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's secretariat shall be provided by the Commission.
3. The Working Party on the Protection of Personal Data shall adopt its own rules of procedure.	4. The Working Party 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.	5. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the reasoned request of a representative of the supervisory authorities, or at the Commission's request.

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.

Article 32

Tasks of the Working Party

1. The Working Party shall:

(a) contribute to the uniform application of the national measures taken under this Directive;

(b) give an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons and on any other proposed measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

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.

2. If the Working Party finds that serious divergences are arising between the laws or practices of Member States concerning the protection of persons with regard to the processing of personal data and that those divergences 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.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be recorded in its minutes and shall be transmitted to the Commission; they may also be transmitted to the advisory committee referred to in Article 34.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be transmitted to the European Parliament and to the Council. The report shall be made public.

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.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

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.

CHAPTER VII

RULE-MAKING POWERS OF THE COMMISSION

Article 33

Exercise of rule-making powers

The Commission shall, in accordance with the procedure laid down in Article 34(2), adopt such technical measures as are necessary to apply this Directive to the specific characteristics of particular sectors or classes of processing, and the measures necessary to ensure the consistent application of this Directive.

Article 34

Advisory Committee

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

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

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.

FINAL PROVISIONS

Article 35

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 1 July 1994.

When Member States adopt these provisions, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. Member States shall set a date after which processing operations which began before 1 July 1994 must be compatible with the national provisions adopted pursuant to this Directive; the date set may be no later than 30 June 1997.

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

3. 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 36

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. The report shall be made public.

Article 37

This Directive is addressed to the Member States.

Done at Brussels,

For the Council

The President

FINANCIAL STATEMENT

Section 1: Financial implications

1. Title of operation: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data

2. Budget headings involved

- A 2510: Expenditure on meetings of committees whose consultation is compulsory in the procedure for drafting Community legislation.

- A 2511: Expenditure on meetings of committees whose consultation is not compulsory in the procedure for drafting Community legislation.

- Titles A1 and A2: Staff and operating expenditure

3. Legal basis

Article 100a of the EEC Treaty

4. Description of operation:

- Objectives:
  - to permit the proper functioning of the internal market by ensuring the free movement of personal data within the Community;
  - to ensure the protection of individuals with regard to personal data.

- Setting-up of two bodies responsible for the protection of individuals with regard to personal data (Articles 31 and 34).

- Persons concerned:

  1. In the case of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 31): representatives of the supervisory authorities of all the Member States (Group 4).

  2. In the case of the Advisory Committee (Article 34): representatives of the Member States (Group 3).

The Advisory Committee will be chaired by a representative of the Commission. The chairman of the Working Party on the Protection of Personal Data will be a member elected for two years. The secretariat of the Advisory Committee and of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data will be provided by the Commission.

5. Classification of expenditure

5.1 Non-compulsory

5.2 Non-differentiated

6. Type of expenditure

- Costs incurred by members attending meetings of the Working Party and the Advisory Committee;

- staff costs.

7. Financial impact on appropriations for operations

None

8. What anti-fraud measures are planned in the proposal for the operation?

None

Section 2: Administrative expenditure (part A of the budget)

1. Will the proposed operation involve an increase in the number of Commission staff? Yes: two C-grade officials.

These posts will be obtained either as part of the allocation of resources decided by the Commission on the basis of future budgets or by internal redeployment.

2. Amount of expenditure involved:

- Secretariat: around ECU 120 000 a year charged to the various budget headings in Titles A1 and A2 (two C officials).

- Meetings of bodies:

  * Working Party on the Protection of Individuals with regard to the Processing of Personal Data:

    24 members (non-governmental) x 4 meetings of 2 days:

- travel expenses: ECU 526.61 x 24 x 4 = ECU 50 555
- allowance for travelling time: ECU 105.40 x 24 x 4 = ECU 10 118
- daily expenses: ECU 105.40 x 24 x 4 x 2 = ECU 20 236

ECU 80 909

* Advisory Committee

24 members (governmental) x 2 meetings of 2 days:

- travel expenses : ECU 526.61 x 24 x 2 = ECU 25 277

Rounded total for a full year:

- secretariat ECU 120 000
- Working Party ECU 81 000
- Advisory Committee ECU 25 000

TOTAL ECU 226 000

Section 3: Elements of cost-effectiveness analysis

1. Objective and coherence with financial programming

Two bodies are to be set up which will be authorized to meet as from 1994. They will be included in the list of committees for the 1994 financial programming.

The timetable for commitment and payment appropriations (non-compulsory, non-differentiated) is as follows:

Commitment appropriations - Payment appropriations

1994	ECU 226 000
1995	ECU 226 000
1996	ECU 226 000
1997	ECU 226 000
1998	ECU 226 000

The appropriations are to be obtained from the various headings of part A under the general budgetary procedure.

2. Grounds for the operation

(a) The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 31)

This Working Party has advisory status and will act independently. It will be composed of representatives of the supervisory authorities of all the Member States.

It will adopt its own rules of procedure. The Working Party's secretariat will be provided by the Commission.

Tasks of the Working Party: see Article 32. It will advise the Commission on any proposed additional measures by giving a completely independent opinion (a fundamental principle in the protection of privacy).

3. Monitoring and evaluation of the operation

3.1 Indicators: analysis of the annual report presented by the Working Party pursuant to Article 32(6).

3.2 Details and frequency: each year on the basis of the above-mentioned report to be presented by the Working Party.

3.3 The main factors of uncertainty will concern the difficulties of harmonizing the different approaches and degrees of experience in the Member States. These differences stem from various factors, e.g. of a cultural or technical nature.

IMPACT ASSESSMENT FORM

THE IMPACT OF THE PROPOSAL ON BUSINESS AND ON OTHER BODIES CONCERNED, WITH SPECIAL REFERENCE TO SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)

Title of proposal: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Reference number:

THE PROPOSAL

1. **Taking account of the principle of subsidiarity, why is Community legislation necessary in this area and what are its main aims?**

Flows of personal data between bodies operating in the various spheres of economic and social activity in the Member States and the processing of such data by those bodies are expanding rapidly precisely because of the completion of the internal market:

- flows between private or public enterprises;
- flows between units which are legally part of the same enterprise;
- flows between national administrations required to provide mutual assistance under various Community instruments;
- flows to medical research centres, etc.

The major differences that exist between national laws (it being borne in mind that four Member States still have no specific laws on data protection: Belgium, Greece, Italy and Spain) give rise to:

- obstacles to the free movement of personal data, particularly in the case of flows to a Member State with no specific laws on the matter, given that the aim of legislation in this area is to protect fundamental rights and freedoms, particularly the privacy of individuals;

- distortions in competition between businesses in the Community, in that some are subject to protective legislation while others are not, depending on the Member State in which they are established.

Moreover, the introduction of rules on data protection is likely to encourage the development of the information market through the legal certainty that these rules provide for the bodies concerned.

Action by the Community is therefore of fundamental importance. It must take the form of an approximation of national laws. The Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, the only instrument of international law in this area, leaves open a wide range of options for applying the principles that it sets out and does not, therefore, allow a sufficient degree of harmonization for the internal market.

THE IMPACT ON BUSINESS, PUBLIC AUTHORITIES AND OTHER BODIES, INCLUDING FOUNDATIONS AND ASSOCIATIONS

2. Who will be affected by the proposal?

The proposal covers, regardless of size or sector of activity, all public and private enterprises, public administrations whose activities are governed by Community law, and foundations and non-profit-making associations in so far as such bodies process personal data (management of suppliers and customers, personnel management, management of members or correspondents of associations and foundations, processing by bodies of data on persons under their administration, provision of information on individuals).

However, as the consultations referred to in point 6 have shown, the areas of industry which will be particularly concerned by the application of this Directive are businesses and bodies in the service sector whose activities are aimed at individuals and are based on the processing of information: direct marketing companies, financial institutions, insurance companies, credit-rating agencies.

3. What will business have to do to comply with the proposal?

Businesses will have to introduce decision-making and organizational procedures that, depending on the structure and size of the concern, involve the head of data processing and organization, the department using such technologies, the legal service and the head of the organization. Where new ways of processing personal data are being designed the organization must, prior to the investment stage:

- check that the proposed forms of data processing are lawful;

- specify the information to be given to data subjects. Such information could be provided on the occasion of the usual contacts between the person in charge of processing (controller) and the data subjects;

- provide for the technical and organizational measures necessary to guarantee the security of data and processing;

- make sure of the notification procedure applicable. After collecting the necessary elements of information, the controller will establish that no notification is necessary, will carry out a simplified formality or will make up a file.

The controller must also ensure that a procedure is in place to handle any requests for right of access by data subjects to data concerning them as well as possible complaints, and take steps to monitor the proper functioning of security measures.

These tasks are to be carried out in the course of new processing operations and can therefore be planned in line with progress in devising the technical processing procedures.

In the case of processing operations carried out before the entry into force of national provisions taken in pursuance of the Directive, such tasks may be planned over a period of three years, as laid down in the Directive.

In the case of bodies established in Member States which already have legislation in this area, the measures required by the Directive do not differ in nature from those already implemented.

In the case of bodies established in Member States which do not have such legislation, methods must be devised although the competent supervisory authorities may be a great help during the launch phase (advice, simplified notification procedure for certain processing operations, etc.).

4. What economic effects is the proposal likely to have?

Protection of individual privacy, as guaranteed by the Directive, will increase social acceptance of the use of the various ways of processing personal data and hence acceptance of their development, this being a factor which will promote growth and job creation in the private and public sectors.

Moreover, these rules on protection are such as to eliminate the distortions of competition arising from the present differences between national laws. As regards international competitiveness, the Directive provides for negotiations with third countries which are still unable to guarantee an adequate level of protection.

5. Does the proposal contain measures to take account of the specific situation of small and medium-sized firms?

No. However, it is reasonable to assume that most processing operations carried out by SMEs will fall into those categories which, depending on the system proposed, could be exempted from the notification requirement or could benefit from a simplified procedure (with completion of these formalities not involving more than a few hours' work). Moreover, the Directive does not provide for any fee for the completion of notification formalities.

CONSULTATION

6. List the organizations which have been consulted about the proposal and outline their main views

(a) Interested parties were consulted primarily through the Economic and Social Committee, which gave a favourable opinion on the proposal (OJ No C 159 of 17 June 1991, p. 38), and through the Committee on Commerce and Distribution (CCD) and the Consumers Consultative Committee.

(b) As regards the amended proposal, direct contacts were held, at the initiative of the Commission departments or business interests concerned, with European business associations with regard to either the horizontal nature of the proposal (UNICE) or the sectors most affected, including the Banking Federation, CELD, FEWITA, GEDIS, the European Federation for Direct Marketing, EAT, CHANGE (non-profit-making bodies), the European Society for Opinion and Marketing Research, ACT, EPC, ENPA, CAEJ, EBU and FAEP (for the press and audiovisual aspects).

The main points raised by the business associations concerning the original proposal were:

- proposal too detailed;

- predominance of the data subject's consent as a condition for the processing of personal data;

- exclusion of any possibility of computerized decision and the preparation of profiles;

- onerous and inappropriate obligations with regard to informing the data subject and notifying the supervisory authorities;

- impossibility of conducting international trade with third countries not guaranteeing an adequate level of protection;

- risk to freedom of expression if some Member States do not proceed with the derogations necessary to reconcile the rules on the exercise of that freedom with those on the protection of privacy.

The amended proposal has attempted to clarify or adapt the text where necessary while continuing to pursue the objective of a high level of protection, without which free movement would not be possible.

ISSN 0254-1475

COM(92) 422 final

DOCUMENTS

EN 06

Catalogue number : CB-CO-92-437-EN-C

ISBN 92-77-47942-6

Office for Official Publications of the European Communities
L-2985 Luxembourg