COM 066

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 14.7.1999
COM(1999) 337 final

99/0153 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data

(presented by the Commission)

EXPLANATORY MEMORANDUM

Community institutions and bodies, and the Commission in particular, handle personal data as part of their everyday work. The Commission exchanges personal data with Member States in implementing the common agricultural policy and the Structural Funds, in administering the customs union and in pursuing other Community policies. In order that data protection might be seamless, the Commission, when it proposed Directive 95/46/EC in 1990, declared that it too would observe the principles it contained.

At the time of its adoption, the Commission and the Council undertook, in a public declaration, to comply with the Directive, and called upon the other Community institutions and bodies to do likewise.

At the time of the Intergovernmental Conference on the review of the Treaty, the question of the application of the rules on data protection to the Community institutions was raised by the Dutch and Greek Governments. At the end of the negotiations, the Treaty signed in Amsterdam inserted in the Treaty establishing the European Community a specific provision on the subject. Numbered Article 286 in the final version, it is worded as follows:

1. *From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.*

2. *Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate.*

Article 286 therefore provides that, from 1 January 1999, Community institutions and bodies will have to apply the Community rules on the protection of personal data laid down for the most part by Directive 95/46/CE, and that the application of those rules will have to be monitored by an independent supervisory body. The present proposal for a Regulation is designed to attain this twin objective.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community and in particular Article 286 thereof,

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the Economic and Social Committee[2],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[3],

Whereas:

(1) Article 286 of the Treaty requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data.

(2) A fullly-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body.

(3) Article 286(2) of the Treaty requires the establishment of an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies.

(4) Article 286(2) of the Treaty requires the adoption of any other relevant provisions as appropriate.

---

1 OJ C
2 OJ C
3 OJ C

(5) A regulation is necessary to provide the individual with legally enforceable rights, to specify the processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory body responsible for the external monitoring of Community processing of data.

(6) The principles of data protection must apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. The principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(7) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community.

(8) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector[5] particularizes and complements Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector.

(9) Various other Community measures, including measures on mutual assistance between national authorities and the Commission, are also designed to particularize and complement Directive 95/46/EC in the sectors to which they relate.

(10) Consistent and homogeneous application of the rules for the protection of individuals, fundamental rights and freedoms with regard to the processing of personal data must be ensured throughout the Community.

(11) The aim is to ensure both effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms and the free flow of personal data between Member States and the Community institutions and bodies or between the Community institutions and bodies for purposes connected with the exercise of their respective competences.

(12) This can best be achieved by adopting measures which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by Community institutions and bodies in the exercise of their competences under the Treaties establishing the European Communities and the Treaty on European Union.

---

[4] OJ L 281, 23.11.1995, p. 31.
[5] OJ L 24, 30.1.1998, p. 1.

(13) The measures must be identical to the provisions laid down in connection with the harmonisation of national laws or the implementation of other Community policies, notably in the mutual assistance sphere. It may be necessary, however, to particularize and complement those provisions when it comes to ensuring protection in the case of the processing of personal data by the Community institutions and bodies.

(14) This holds true for the rights of the individuals whose data are being processed, for the obligations of the Community institutions and bodies doing the processing, and for the powers to be vested in the independent supervisory body responsible for ensuring that this Regulation is properly applied.

(15) Processing of personal data for the performance of the tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.

(16) It may be necessary to monitor the computer networks operated under the control of the Community institutions and bodies for the purposes of prevention of unauthorised use. The European Data Protection Supervisor should determine whether and under what conditions that is possible.

(17) Under Article 21 of Council Regulation (EC) No 322/97 of 17 February 1997 on Community statistics[6], that Regulation is to apply without prejudice to Directive 95/46/EC.

(18) For reasons of transparency, it is necessary to make public further information on the application of this Regulation, including a list of the Community institutions and bodies which are subject to this Regulation.

(19) The Working Party on the Protection of Individuals with regard to the processing of personal data set up under Article 29 of Directive 95/46/EC has delivered its opinion,

HAVE ADOPTED THIS REGULATION:

---

[6] OJ L 52, 22.2.1997, p. 1.

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Regulation

1. In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as Community institutions or bodies, shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. The independent supervisory body established by this Regulation, hereinafter referred to as European Data Protection Supervisor, shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body.

Article 2

Definitions

For the purposes of this Regulation:

(a) "personal data" shall mean 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/her physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, 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 filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(d) "controller" shall mean the Community institution or body, the Directorate General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific

Community act, the controller or the specific criteria for its nomination may be designated by such Community act;

(e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) "third party" shall mean any natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

(g) "recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) "the data subject's consent" shall mean any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed;

Article 3

Scope

1. This Regulation shall apply to the processing of personal data by all Community institutions and bodies.

2. This Regulation 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 form part of a filing system or are intended to form part of a filing system.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

SECTION 1

PRINCIPLES RELATING TO DATA QUALITY

Article 4

1. Personal data must be:

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data shall only be processed for such purposes;

   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use, in particular with regard to making them anonymous.

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

SECTION 2

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 5

Lawfulness of processing

Personal data may be processed only if:

(a) processing is necessary for the performance of a task carried out in the public interest on the basis of a law or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or

(b) processing is necessary for compliance with a legal obligation to which the controller is subject, or

(c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

(d) the data subject has unambiguously given his/her consent, or

(e) processing is necessary in order to protect the vital interests of the data subject.

Article 6

Further processing for compatible purposes

1. Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

2. Personal data collected for other purposes may be processed to ensure compliance with financial and budgetary regulations.

3. Personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the purposes referred to in Article 18(1)(a).

Article 7

Transfer of personal data within or between Community institutions or bodies

1. Personal data shall only be transmitted within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient.

2. The controller and the recipient shall bear the responsibility for the legitimacy of the transmission.

   The controller shall only verify the competence of the recipient and the merits of the request. If doubts arise as to the merits, the controller shall, however, also check the necessity of the transmission.

   The recipient shall ensure that the necessity of the transmission can be subsequently verified.

Article 8

Transmissions to persons and bodies, other than Community institutions and bodies, located in the Member States

1. Personal data shall only be transmitted to persons and bodies located in the Member States if the recipient established the necessity of having the data communicated and if no reasons exist to assume that the data subject's legitimate interests might be prejudiced.

2. The recipient shall process the personal data only for the purposes for which they were transmitted.

Article 9

Transfer of personal data to persons and bodies, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

1. Personal data shall only be transferred to persons and bodies other than Community institutions and bodies, which are not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transmitted strictly within the range of tasks covered by the competence of the controller and the requirements mentioned in Article 4(1)(b) of this Regulation are fulfilled.

2. The adequacy of the level of protection afforded by the country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations;

particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country or international organisation of final destination, the rules of law, both general and sectoral, in force in the country or international organisation in question and the professional rules and security measures which are complied with in that country or international organisation.

3. The Community institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission, assisted by the committee set up by Article 31(1) of Directive 95/46/EC, finds that a country or an international organisation ensures or does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, the Community institutions and bodies shall take the necessary measures to comply with the Commission's decision.

That decision shall be adopted in accordance with the management procedure laid down in Article 4 of Council Decision 1999/468/EC[7] and without prejudice to Article 8 thereof.

The period provided for in Article 4(3) of Decision 1999/468/EC shall be three months.

5. By way of derogation from paragraph 1, the Community institution or body may transfer personal data if:

(a) the data subject has given his/her consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to Community law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can

[7] OJ L 184, 17.7.1999, p. 23.

demonstrate legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case.

6. The Community institutions and bodies shall inform the European Data Protection Supervisor of (categories of) cases where they have applied paragraph 5.

SECTION 3

THE PROCESSING OF SPECIAL CATEGORIES OF DATA

Article 10

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, shall be prohibited.

2. Paragraph 1 shall not apply where:

   (a) the data subject has given his/her explicit consent to the processing of those data, except where the internal rules of the Community institution or body provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his/her consent; or

   (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment in so far as it is authorised by Community law or rules implementing Community law, or agreed upon by the European Data Protection Supervisor, providing for adequate safeguards; or

   (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent; or

   (d) processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims; or

   (e) processing is carried out in the course of its legitimate activities with appropriate guarantees by a non-profit seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, assessment of the medical aptitude for recruitment, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by decision of the European Data Protection Supervisor.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by Community law or other legal instruments adopted on the basis of the EU Treaty laying down suitable specific safeguards or authorised by the European Data Protection Supervisor.

6. The European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application in a Community institution or body may be processed.

SECTION 4

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 11

Information in cases of collection of data from the data subject

1. The controller must provide a data subject from whom data relating to himself/herself are collected with at least the following information, except where he/she already has it:

   (a) the identity of the controller;

   (b) the purposes of the processing for which the data are intended;

   (c) the recipients or categories of recipients of the data;

   (d) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

   (e) the existence of the right of access to and the right to rectify the data concerning him/her;

   (f) any further information such as:

   - the legal basis of the processing for which the data are intended,

- the time-limits for storing the data,

- the right to have at any time recourse to the European Data Protection Supervisor,

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

2. By way of derogation from paragraph 1, the provision of information or part of it may be deferred as long as this is necessary to attain the legitimate objective of a statistical survey in view of its subject or its nature. The information must be provided as soon as the reason for which the information is withheld ceases to exist, unless this is manifestly unreasonable or impracticable. In such cases, the information shall be provided as soon as those circumstances have disappeared at a later stage.

Article 12

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, the controller must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he/she already has it:

   (a) the identity of the controller;

   (b) the purposes of the processing;

   (c) the categories of data concerned;

   (d) the recipients or categories of recipients;

   (e) the existence of the right of access to and the right to rectify the data concerning him/her;

   (f) any further information such as:

   - the legal basis of the processing for which the data are intended,

   - the time-limits for storing the data,

   - the right to have at any time recourse to the European Data Protection Supervisor,

   - the origin of the data, except where the controller can not disclose this information for reasons of professional secrecy,

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Community law. In these cases the Community institution or body shall provide for appropriate safeguards.

SECTION 5

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 13

Right of access

Every data subject shall have the right to obtain at any time without excessive delay and free of charge from the controller:

(a) confirmation as to whether or not data related to him/her are being processed;

(b) information as to the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the data are disclosed;

(c) communication in an intelligible form of the data undergoing processing and of any available information as to their source;

(d) knowledge of the logic involved in any automated decision process concerning him/her.

Article 14

Rectification

The controller shall at the request of the data subject rectify without delay inaccurate or incomplete personal data.

Article 15

Blocking

1. Personal data shall be blocked where:

   (a) their accuracy is contested by the data subject and neither their accuracy nor their inaccuracy can be ascertained;

   (b) the controller no longer needs them for the accomplishment of his/her tasks but they have be maintained for reasons of proof;

   (c) the processing was unlawful and the data subject opposes their erasure and demands instead their blocking.

2. In automated filing systems blocking shall in principle be ensured by technical means. The fact that the personal data are blocked shall be indicated in the system in such a way that it becomes clear that the personal data cannot be used.

3. Blocked personal data shall, with the exception of their storage, only be processed if they are required for discharging the burden of proof, where the data subject has consented, or for reasons based on the legal interest of a third party.

Article 16

Erasure

1. Personal data shall be erased if their processing was unlawful, in particular when the provisions of Sections 1, 2 and 3 of Chapter II are violated.

2. Personal data shall be erased if the controller no longer needs them for the accomplishment of his/her tasks and there is no reason to believe that the data subject's interests might be prejudiced by the erasure.

Article 17

Notification to third parties

The controller shall notify third parties to whom the data have been disclosed of any rectification, erasure or blocking unless this proves impossible or involves a disproportionate effort.

SECTION 6

EXEMPTIONS AND RESTRICTIONS

Article 18

1. The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Article 13, Article 33 and Article 34(1) when such a restriction constitutes a necessary measure to safeguard:

   (a) the prevention, investigation, detection and prosecution of criminal offences;

   (b) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

   (c) the protection of the data subject or of the rights and freedoms of others;

   (d) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a) and (b).

2. Articles 13 to 16 shall not apply when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics, provided that there is clearly no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards, in particular to ensure that the data are not used for taking measures or decisions regarding a particular individual.

3. If a restriction as provided for by paragraph 1 is applied, the data subject shall be informed of the major reasons on which the application of the restriction is based and of his/her right to have recourse to the European Data Protection Supervisor.

4. As soon as the reason for which the restrictions as provided for by paragraph 1 are applied ceases to exist, the provisions referred to in paragraph 1 shall again be fully applied.

SECTION 7

OBJECTIONS AND COMPLAINTS

Article 19

The data subject's right to object

The data subject shall have the right to object at any time on compelling legitimate grounds relating to his/her particular situation to the processing of data relating to him/her, except in the cases covered by Article 5, points (b), (c) and (d). Where there is a justified objection, the processing in question may no longer involve those data.

Article 20

The data subject's right to lodge complaints

The data subject shall have the right to lodge complaints at any time to the European Data Protection Supervisor.

Article 21

Automated individual decisions

No one shall be subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, reliability or conduct, unless the decision is expressly authorised by a legal provision which also lays down measures to safeguard the data subject's legitimate interests.

SECTION 8

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 22

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself/herself, who has access to personal data shall not process them except on instructions from the controller, unless he is required to so by national law.

Article 23

Security of processing

1. Having regard to the state of the art and the cost of their implementation, the controller shall implement the technical and organisational measures necessary to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

2. Where personal data are manually processed, appropriate measures shall be taken in particular to prevent any unauthorised access or disclosure, alteration, destruction or accidental loss.

3. Where personal data are processed by automated means, measures shall be taken in particular to:

   (a) prevent any unauthorised person from gaining access to computer systems processing personal data;

   (b) prevent any unauthorised reading, reproduction, alteration or removal of storage media;

   (c) prevent any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;

   (d) prevent unauthorised persons from using data processing systems by means of data transmission facilities;

   (e) ensure that authorised users of a data processing system can access no personal data other than those to which their access right refers;

   (f) record which personal data have been communicated, at what times and to whom;

(g) ensure that it will be subsequently possible to check and verify which personal data have been processed, at what times and by whom;

(h) ensure that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;

(i) ensure that, during communication of personal data and during transport of storage media, the data cannot be read, copied, or erased without authorisation;

(j) design the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.

Article 24

Processing of personal data on behalf of controllers

1. The controller shall, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures required by Article 23 and shall ensure compliance with those measures.

2. The carrying out of processing by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

   (a) the processor shall act only on instructions from the controller;

   (b) the obligations set out in Article 23 shall also be incumbent on the processor.

3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 23 shall be in writing or in another equivalent form.

SECTION 9

DATA PROTECTION OFFICER

Article 25

Appointment and tasks of the Data Protection Officer

1. Each Community institution and Community body shall appoint at least one person of appropriate rank as personal data protection officer, with the task of:

(a) ensuring that controllers and data subjects are informed of their rights and obligations;

(b) cooperating with the European Data Protection Supervisor at the latter's request or on his/her own initiative;

(c) ensuring in an independent manner the internal application of provisions of this Regulation and of all other provisions adopted to implement these rules;

(d) keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 26(2);

(e) notifying the European Data Protection Supervisor of the processing operations likely to present specific risks within the meaning of Article 28;

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

2. The Data Protection Officer shall be provided with the staff and resources required for the performance of his/her duties.

3. Further implementing rules concerning the Data Protection Officer shall be adopted by each Community institution or body on the basis of the guidelines laid down in Annex I. The implementing rules shall in particular concern the qualifications, the appointment, dismissal, independence and the tasks, duties and powers of the Data Protection Officer.

Article 26

Notification to the Data Protection Officer

1. The controller shall give prior notice to the Data Protection Officer of any processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. The information to be given shall include at least the information referred to in Annex II.

Any change affecting that information shall be notified promptly to the Data Protection Officer.

Article 27

Register

A register of processing operations notified in accordance with Article 26 shall be kept by each Data Protection Officer.

The registers shall contain at least the information referred to in Article 26(2).

The registers may be inspected by any person.

SECTION 10

PRIOR CHECKING BY THE EUROPEAN DATA PROTECTION SUPERVISOR

Article 28

1. The European Data Protection Supervisor shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies.

   These processing operations shall include the following:

   - certain processing operations involving special categories of data as referred to in Article 10;

   - processing operations intended to assess the personality of the data subject, including his/her ability, efficiency and conduct.

   These processing operations shall be subject to prior checks.

2. The prior checks shall be carried out by the European Data Protection Supervisor following receipt of a notification from the Data Protection Officer who, in case of doubt, shall consult the European Data Protection Supervisor.

3. The European Data Protection Supervisor shall deliver his/her opinion within two months following receipt of the notification. If the opinion has not been delivered by the end of that two-month period, it shall be deemed to be favourable.

4. The European Data Protection Supervisor shall keep a register of all processing operations that have been notified to him/her pursuant to paragraph 2. The register shall contain the information referred to in Article 26(2). It shall be open to public inspection.

5. Automated means of communication between the Community institutions or bodies such as an on-line access to databases or an interlinking shall only be established after examination by the European Data Protection Supervisor.

In the course of the examination, the European Data Protection Supervisor shall determine whether an automated communication is compatible with the legitimate interests of the data subjects and necessary in view of the tasks of the Community institutions or bodies involved.

CHAPTER III

REMEDIES AND SANCTIONS

Article 29

Remedies

1. Without prejudice to any judicial remedy, every data subject may complain to the European Data Protection Supervisor if he/she considers that his/her rights have been violated as a result of the processing of his/her personal data by a Community institution or body.

2. The Court of Justice of the European Communities and the Court of First Instance of the European Communities shall have jurisdiction to hear all disputes which relate to the provisions of this Regulation, including claims for damages.

Article 30

Sanctions

Any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his/her part, shall make an official or other servant of the European Communities liable to disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the Communities or in the conditions of employment applicable to them.

CHAPTER IV

PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF INTERNAL TELECOMMUNICATIONS NETWORKS

Article 31

Scope

In addition to the other provisions of this Regulation, this Chapter shall apply to the processing of personal data in connection with the use of telecommunications networks and terminal equipment operated under the control of a Community institution or body.

For the purpose of this Chapter, 'user' shall mean any natural person using a telecommunications network operated under the control of a Community institution or body.

Article 32

Security

1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services and/or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform the users concerning such risks and any possible remedies or alternative means of communication.

Article 33

Confidentiality of the communications

1. Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment.

Listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, shall be prohibited.

2. Paragraph 1 shall not affect any recording of communications authorised by the internal rules of the Community institutions or bodies, for the purpose of providing evidence of legal or procedural acts relevant to the official tasks of the Community institutions or bodies concerned, subject to the agreement of the European Data Protection Supervisor.

Article 34

Traffic and billing data

1. Traffic data relating to users processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications system, traffic data as indicated in a list agreed by the European Data Protection Supervisor may be processed.

3. Processing of traffic and billing data shall be restricted to what is necessary for the purposes of the activities referred to in paragraph 2 and shall only be carried out by persons handling billing, traffic or budget management.

4. Users of the telecommunication networks shall have the right to receive non-itemised bills.

Article 35

Directories of users

1. Personal data contained in printed or electronic directories of users shall be limited to what is necessary for the specific purposes of the directory.

2. The Community institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for direct marketing purposes.

Article 36

Presentation and restriction of calling and connected line identification

1. Where presentation of calling-line identification is offered, the calling user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification.

2. Where presentation of calling-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to prevent the presentation of the calling line identification of incoming calls.

3. Where presentation of connected line identification is offered, the called user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

4. Where presentation of calling and/or connected line identification is offered, the Community institutions and bodies shall inform the users thereof and of the possibilities set out in paragraphs 1, 2 and 3.

Article 37

Exceptions

Community institutions and bodies shall ensure that there are transparent procedures governing the way in which they may override the elimination of the presentation of calling line identification:

(a) on a temporary basis, upon application of a user requesting the tracing of malicious or nuisance calls;

(b) on a per-line basis for organisational entities dealing with emergency calls, for the purpose of answering such calls.

CHAPTER V

SUPERVISORY AUTHORITY: EUROPEAN DATA PROTECTION SUPERVISOR

Article 38

Supervisory authority: European Data Protection Supervisor

1. A supervisory authority is hereby established referred to as the European Data Protection Supervisor.

2. It shall be responsible for monitoring the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or a Community body.

Article 39

Appointment

1. On a proposal from the Commission, the European Parliament, the Council and the Commission shall appoint by common accord the European Data Protection Supervisor for a term of four years.

2. The European Data Protection Supervisor shall be chosen from among persons who belong or have belonged in their respective countries to the independent authorities supervising the processing of personal data or who are especially qualified for this office.

3. The European Data Protection Supervisor shall be eligible for reappointment.

4. The European Data Protection Supervisor shall remain in office until he/she has been replaced.

5. Apart from normal replacement or death, the duties of the European Data Protection Supervisor shall end when he/she resigns, or is compulsory retired in conformity with paragraph 6.

6. The European Data Protection Supervisor may be dismissed by the Court of Justice at the request of the European Parliament, the Council or the Commission, if he/she no longer fulfils the conditions required for the performance of his/her duties or if he/she is guilty of serious misconduct.

7. Subject to the provisions of this Chapter, the provisions of the Protocol on the Privileges and Immunities of the European Communities applicable to the Judges of the Court of Justice shall also apply to the European Data Protection Supervisor.

Article 40

Conditions of employment

1. The European Parliament, the Council and the Commission shall by common accord determine the conditions of employment of the European Data Protection Supervisor and in particular his/her salary, allowances and any other benefits in lieu of remuneration.

2. The European Parliament shall ensure that the European Data Protection Supervisor is provided with the staff and equipment necessary for the performance of his/her tasks.

3. The staff and equipment to be provided shall be itemised in a separate Chapter to the budget of the European Parliament.

4. Staff members shall be appointed by the European Data Protection Supervisor. Their superior shall be the European Data Protection Supervisor and they shall be subject exclusively to his/her direction.

5. The officials and the other staff members shall be subject to the rules and regulations applicable to officials and other servants of the European Communities.

6. In matters concerning its staff, the European Data Protection Supervisor shall have the same status as the institutions within the meaning of Article 1 of the Staff Regulations of Officials of the European Communities.

Article 41

Independence

1. The European Data Protection Supervisor shall act in complete independence in the performance of his/her duties.

2. The European Data Protection Supervisor shall, in the performance of his/her duties, neither seek nor take instruction from anybody.

3. The European Data Protection Supervisor shall refrain from any action incompatible with his/her duties and shall not, during his/her term of office, engage in any other occupation, whether gainful or not.

4. The European Data Protection Supervisor shall, after his/her term of office, behave with integrity and discretion as regards the acceptance of appointments and benefits.

Article 42

Professional secrecy

The European Data Protection Supervisor and his/her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential matters which have come to their knowledge in the course of the performance of their official duties.

Article 43

Duties

The European Data Protection Supervisor shall:

(a) receive and investigate complaints;

(b) supervise all processing operations involving personal data by any Community institution or body with the exception of the Court of Justice and the Court of First Instance acting in their judicial role;

(c) advise all Community institutions and bodies on all matters concerning the use of personal data, in particular before they draw up internal rules relating to the protection of individual rights and freedoms with regard to the processing of personal data;

(d) follow the development of information and communication technologies insofar as they have an impact on the protection of personal data;

(e) cooperate with the national supervisory authorities to the extent necessary for the performance of his/her duties, in particular by exchanging all useful information or requesting an authority of a Member State to exercise its powers;

(f) participate in the activities of the Working party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;

(g) keep a register of processing notified to him/her;

(h) carry out a prior check of processing notified to him/her.

Article 44

Consultation

1. The Community institutions and bodies shall inform the European Data Protection Supervisor when drawing up draft measures related to the processing of personal data involving a Community institution or body alone or jointly with others.

2. The European Data Protection Supervisor shall be informed by the Commission of all draft proposals for Community legislation entailing a processing of personal data.

3. The European Data Protection Supervisor may be consulted by each Community institution or body on all operations related to the processing of personal data.

Article 45

Recourse

1. Any person employed with Community institutions or bodies may on a matter affecting his/her tasks have recourse to the European Data Protection Supervisor, without acting through official channels.

2. No one shall suffer prejudice on account of a recourse or a complaint to the European Data Protection Supervisor alleging a violation of the provisions governing the processing of personal data.

Article 46

Powers

1. The European Data Protection Supervisor shall, in particular:

   (a) conduct inquiries either on his/her own initiative or on the basis of complaints or recourses;

   (b) be supplied without delay with all information concerning his/her enquiries;

   (c) be granted at any time access to all official premises.

   All controllers shall support the European Data Protection Supervisor in the performance of his/her duties.

2. The European Data Protection Supervisor shall have the power to:

   (a) order the rectification, blocking erasure or destruction of all data processed in violation of the provisions governing the processing of personal data;

   (b) impose a temporary or definitive ban on processing;

   (c) warn or admonish the controller;

   (d) report the matter to the Community institution or body concerned and if necessary to the European Parliament, the Council and the Commission;

   (e) intervene in actions brought before the Court of Justice and the Court of First Instance;

   (f) give advice to the data subjects and, if requested, assist them as expert in proceedings before the Court of First Instance.

3. Where the European Data Protection Supervisor establishes a violation of the provisions governing the processing of personal data, or any other irregularities in the processing, he/she shall refer the matter to the Community institution or body concerned and where appropriate make proposals for remedying those irregularities and for improving the protection of the data subjects.

4. The Community institution or body concerned shall inform the European Data Protection Supervisor of its views within a period to be specified by him/her. The reply shall also include a description of the measures taken in response to the remarks of the European Data Protection Supervisor.

5. In the event of a complaint or recourse, the European Data Protection Supervisor shall inform the persons concerned of the outcome of his/her enquiries.

6. Where the data subject has been denied access, the European Data Protection Supervisor shall only inform him/her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made.

   If the European Data Protection Supervisor considers that the application of the restriction to the right of confirmation provided for in Article 13(a), is deprived of its effect by providing this information, the European Data Protection Supervisor shall not inform the data subject of the outcome of his/her enquiry.

7. Actions against decisions of the European Data Protection Supervisor shall be brought before the Court of Justice or the Court of First Instance.

Article 47

Activities report

1. The European Data Protection Supervisor shall submit an annual report on his/her activities to the European Parliament and at the same time make it public.

2. The report shall be forwarded to the other institutions and bodies of the European Union and shall be discussed by the European Parliament together with their replies.

CHAPTER VI

FINAL PROVISIONS

Article 48

Transitional period

Community institutions and bodies shall ensure that processing already under way on the date this Regulation enters into force is brought into conformity with this Regulation within one year of that date.

Article 49

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Communities*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

Annex I

1. The data protection officer shall be selected on the basis of his/her authority, his/her expert knowledge of data protection and his/her personal reliability.

2. The appointment of the data protection officer shall not entail a conflict of interests with regard to other official duties, in particular in relation to the application of the provisions of this Regulation.

3. The data protection officer shall be appointed for a term of at least two years. He/she shall be eligible for reappointment. The data protection officer may only be dismissed with the consent of the European Data Protection Supervisor, if he/she no longer fulfils the conditions required for the performance of his/her duties.

4. With respect to the performance of his/her duties, the data protection officer may not receive any instructions.

5. After his/her appointment the data protection officer shall be registered with the European Data Protection Supervisor by the institution, body (or person) which appointed him/her.

6. The data protection officer may make recommendations for the practical improvement of data protection and advise the Community institution or body which appointed him/her and the controller concerned on matters concerning the application of data protection provisions. Furthermore he/she shall, on his/her own initiative or at the request of the Community institution or body which appointed him/her, the controller, the Staff Committee concerned or data subject, investigate matters and occurrences directly relating to his/her tasks and come to his/her notice.

7. The data protection officer may be consulted by the Community institution or body which appointed him/her, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation.

8. No one shall suffer prejudice on account of a matter brought to the attention of the data protection officer and suggesting a violation of the provisions of this Regulation.

9. Every controller concerned shall be required to assist the data protection officer in performing his/her duties and to give information in reply to questions. In performing his/her duties, the data protection officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data processing installations and data carriers, and may collect the necessary information.

10. To the extent required, the data protection officer shall be relieved from other activities. The data protection officer and his/her staff, to whom Article 287 of the Treaty shall apply, shall be required not to divulge information or documents which they obtain in the course of their duties.

Annex II

1. The name and address of the controller.

2. The names of the persons and/or the indication of the organisational parts of an institution or body charged with the processing of personal data for a particular purpose.

3. The purpose or purposes of the processing.

4. A description of the category or categories of data subjects and of the data or categories of data relating to them.

5. The legal basis of the processing for which the data are intended.

6. The recipients or categories of recipient to whom the data might be disclosed.

7. The time limits for blocking and erasure of the different categories of data.

8. Proposed transfers of data to third countries.

9. A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 23 to ensure security of processing.

COMMENTS ON THE ARTICLES

By virtue of the new Article 286 of the EC Treaty the Community institutions and bodies will be bound to apply the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data. This obligation substantially limits the freedom of choice for the Commission as to the contents and scope of the substantive data protection rules which are laid down in this Regulation. In other words, Article 286 of the EC Treaty obliges the Commission to respect the limits set by Directive 95/46/EC. This is the main reason why this Regulation closely follows the wording and system of Directive 95/46/EC. The other reason is the need for equal interpretation of the Directive and the Regulation.

The wording of the Regulation is however not completely identical to that of the Directive. The Directive establishes a framework that requires further implementation, either in national law, for the Member States, or in this Regulation for the Community institutions and bodies. Thus the rules laid down in this Regulation are more precise and detailed than those of the Directive. On certain issues the Directive opens the possibility to choose between different alternatives. This is another reason why the wording of the Regulation is different from that of the Directive. In addition the Regulation establishes the independent supervisory authority referred to in Article 286 of the EC Treaty, which requires more detailed provisions than those of the Directive which leave the implementation to the national law of the Member States.

The comments concentrate on those provisions of the Regulation which are not identical to their counterparts in the Directive.

Chapter I: General provisions

Article 1: Object of the Regulation

Article 1 concerns the object of the Regulation. The protection afforded extends not only to the processing of data on employees of the institutions or on any other person working on behalf of the institutions, but also to the processing of data on any natural person external to the institutions, such as suppliers or persons in receipt of monies from Community funds. Personal information transmitted by Member States to the Commission in connection with the management or monitoring of the payment of Community subsidies is, in particular, protected under this Regulation.

It should be noted that the object of the present Regulation is different from that of the Directive.

The Directive, which is based on Article 100a of the EC Treaty, seeks to reconcile the requirements underlying the establishment of the single market with those underlying the protection of individuals. This is expressed in the two paragraphs of Article 1: the first laying down the obligation for Member States to protect the rights and freedoms of individuals in accordance with the Directive, and the second drawing the necessary consequences from the point of view of the free flow of personal data in the single market. In other words, the first paragraph has to do with the means employed,

namely harmonisation of national law, and the second with the objective pursued, namely the free flow of personal data.

There is no need to reproduce these considerations in Article 1 of the present Regulation.

The Regulation is intended to implement the obligation incumbent on Community institutions and bodies to protect individuals' fundamental rights and freedoms, and in particular their right to privacy with respect to processing of their personal data.

It will clearly have the effect, therefore, of ensuring that personal data transmitted, for the purpose of the performance of their duties, to Community institutions and bodies will be dealt with under conditions ensuring respect for the fundamental rights and freedoms of the data subjects, those conditions being themselves aligned on those laid down in the Directive.

It is not necessary, however, to repeat in the present Regulation a provision similar to Article 1(2) of the Directive, the free flow of information, including personal data, between Member States and Community institutions and bodies or between those institutions and bodies being governed by the relevant provisions of the Treaties (such as Article 213 of the EC Treaty) and of secondary legislation.

It goes without saying that the present Regulation is without prejudice to rights which may be guaranteed by other provisions, Community and national. This is the case in particular with the rules laid down by the Staff Regulations of Officials of the European Communities.

Article 2: Definitions

This Article reproduces the definitions in Article 2 of the Directive.

The definition of "controller" has, however, been adapted to fit the specific Community context. The changes are purely factual in nature, being intended to show that, depending on the circumstances, the controller may be an institution, a body or an administrative unit such as a Directorate-General. The criteria for determining who is actually to be considered the controller of data - this being the entity which decides on the purposes and means of processing - are, however, taken from the Directive.

Article 3: Scope

Paragraph 1: institutions and bodies to which the Regulation applies

The Regulation applies to the processing of personal data by all Community institutions and bodies. It therefore covers processing by:

- the institutions listed in Article 7 of the EC Treaty as amended by the Treaty on European Union, namely the European Parliament, the Council, the Commission, the Court of Justice and the Court of Auditors;

- the bodies created by the Treaties establishing the European Community, the European Coal and Steel Community and Euratom, namely the European Central Bank, the European Investment Bank, the Ombudsman, the Economic and Social Committee and the Committee of the Regions;

- bodies set up under secondary Community legislation based on, say, Article 308 EC, such as the European Centre for the Development of Vocational Training; the European Foundation for the Improvement of Living and Working Conditions; the European Environment Agency; the European Training Foundation; the European Monitoring Centre for Drugs and Drugs Addiction; the European Agency for the Evaluation of Medicinal Products; the Office of Harmonisation in the Internal Market (Trade Marks and Designs); the European Agency for Safety and Health at Work; the Community Plant Variety Office; the Translation Centre for the bodies of the Union.

The Regulation applies to processing carried out in the course of all activities of Community institutions and bodies. No distinction is made between those activities: they may be activities carried on under the EC Treaty, the ECSC Treaty or the Euratom Treaty, or even, where appropriate, under Title VI of the Union Treaty.

On the other hand, the Regulation's scope does not extend to the processing of personal data by bodies set up under Title VI of the Union Treaty, such as Europol.

Paragraph 2: processing subject to the Regulation

This paragraph reproduces Article 3(1) of the Directive: it applies to the processing of data wholly or partly by automatic means, and to the processing otherwise than by automatic means of data which form part, or are intended to form part, of a filing system.

Chapter II: General rules on the lawfulness of the processing of personal data

Section I: Principles relating to data quality

Article 4

This Article reproduces the provisions of Article 6 of the Directive.

It reproduces in particular, in subparagraphs (b) and (c), the derogations permitting the subsequent use of data for historical, statistical or scientific purposes, which derogations must, however, be accompanied by appropriate safeguards.

The Article provides that the appropriate safeguards must provided down by the institution or body pursuing the historical, statistical or scientific purpose concerned.

The further processing for other purposes than those for which the data originally have been collected may be expressly authorised by legal provisions, such as Article 16 of Council Regulation (EC) No 322/97 of 17 February 1997 on Community Statistics, which provides for the use of administrative data in order to reduce response burdens on respondents.

Section II: Criteria for making data processing legitimate

Article 5

This Article contains, like Article 7 of the Directive, an exhaustive list of the criteria for making processing legitimate.

Three changes are made, however:

- the list is presented differently;
- the list is shorter;
- the wording of one of the criteria is made more explicit.

- The list is presented differently: the criteria have been listed in the order of practical importance that can reasonably be expected in the case of public authorities such as Community institutions and bodies. In particular, it is only logical to place at the top of the list the performance of the task carried out by those institutions and bodies. By the same token, even if they are necessary for the purpose of carrying out certain activities of the institutions and bodies, e.g. the running of their medical services, the data subject's consent or vital interests should not in practice be the criteria most often applied in order to make processing legitimate.

- The list is shorter: point (f) of Article 7 of the Directive has not been included in the Regulation. This point, which bases the legitimacy of the processing on the legitimate interests of the controller or of a third party, except where such interests are overridden by the interests of the data subject, is not applicable to public-sector activities. On the contrary, its wide scope should cover only private-sector activities.

- The alteration of the wording of point (a): this point reproduces point (e) of Article 7 of the Directive, adapting it to suit the Community context: it is in Community institutions and bodies that official authority on the basis of which data may be processed is vested. Point (a) also includes the processing of personal data necessary for the daily management of the institutions and bodies, e.g. the processing of personal data of officials.

Article 6: Further processing for compatible purposes

This Article refers to the processing of data for a purpose which, though different, is compatible with the purpose for which the data were collected.

Paragraph 1 requires legitimisation of further processing for compatible purposes by the internal rules of the institution or body concerned.

Paragraphs 2 and 3 specify two situations of further processing. Paragraph 2 allows further processing to ensure compliance with financial and budgetary regulations. Paragraph 3 prohibits further processing of personal data collected for the security or control of the processing systems or operations.

Article 6 applies without prejudice to Article 18 which lays down the conditions under which further processing for incompatible purposes can be considered permissible.

Articles 7, 8 and 9: Transfer of personal data

The Articles 7, 8 and 9 distinguish between three different situations.

Article 7 deals with the transfer of personal data from one institution or body to another and with transfers within the institutions and bodies. In this situation personal data are transferred to a recipient who is also subject to this Regulation.

Article 8 deals with the transfer of personal data from a Community institution or body to a recipient who is subject to the provisions of Directive 95/46/EC.

Articles 7 and 8 apply without prejudice to Articles 4, 5 and 6. They contain additional safeguards and in case of Article 7 specify the responsibility of the controller and the recipient.

Article 9: Transfer of personal data to a recipient not subject to an adequate level of protection

Article 9 reproduces Articles 25 and 26 of the Directive and deals with the transfer of personal data to a recipient who is neither subject to this Regulation nor to Directive 95/46/EC. The majority of cases will concern the transfer of personal data to third countries. The procedural provisions of Article 9 are where possible designed in line with those of the Directive.

Section III: Special categories of processing

Article 10: The processing of special categories of data

The structure of this Article is the same as that of Article 8 of the Directive in that it contains:

- first, in paragraph 1, a prohibition on the processing of sensitive data, whereby the following categories of data are deemed to be sensitive: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life;

- and, secondly, a series of derogations meeting specific needs and coupled with appropriate safeguards.

It should be noted that the Staff Regulations of Officials of the European Communities already contain provisions prohibiting the inclusion in officials' personal files of certain sensitive data. Article 26 of the Staff Regulations mentions officials' political, philosophical or religious views. The other categories of data considered sensitive by the Directive are not referred to in the Staff Regulations, which, when the time comes, will have to be aligned on the present Regulation.

The derogation from the processing of data relating to criminal convictions referred to in Article 8(5) of the Directive can apply only partially to Community institutions and bodies.

The Community supervisory authority is empowered by paragraphs 4 to 6 to take decisions on additional exemptions (paragraph 4), to authorise processing of data relating to offences, criminal convictions and security measures (paragraph 5), and to determine the conditions under which a personal number or other identifier may be processed within a Community institution or body (paragraph 6).

An example of processing of personal data which can be authorised by the European Data Protection Supervisor is the processing to prevent the unauthorised use of computer networks, e.g. because they are used to distribute racist political material or pornography.

The discretion granted to the European Data Protection Supervisor in paragraphs 4 to 6 cannot be used in a way contrary to the exemptions laid down in Community law or other legal instruments.

Lastly, it is proposed that no use be made in this Regulation of the option given by the Directive to Member States under Article 8(5), second subparagraph, extending to administrative sanctions and judgments in civil cases the arrangements applicable to criminal sanctions.

Section IV: Information to be given to the data subject

Article 11: Information in cases of collection of data from the data subject

Article 11(1) is closely modelled on Article 10 of the Directive.

Two comments are called for, however:

as regards the party by whom the information is to be supplied: the reference to the representative of the controller in Article 10 of the Directive relates to the situation whereby the controller is established, not in the Community, but in a non-Community country. Such a reference is not pertinent in the case of Community institutions and bodies and has therefore not been included in this Regulation.

as regards the list of information to be given to the data subject: like Article 10 of the Directive, Article 11 of this Regulation contains a list of such information. It is proposed that the minimum list in the Directive be expanded.

Article 10 of the Directive does not explicitly specify at which moment in time the data subject is to be informed. In general this will be the moment when the personal data are collected. Article 11(2) allows deferment of the provision of information to a later moment if necessary for the specific reason mentioned in this provision.

Article 12: Information where the data have not been obtained from the data subject

The comments on Article 11 also hold true for Article 12. The exceptions to the information obligation in Article 11 of the Directive have been reproduced, the law which can serve as a basis for such a derogation being Community law.

Section V: The data subject's right of access to data

In the interests of greater clarity; the contents of Article 12 of the Directive have been split up and reproduced in Articles 13 to17.

The wording has also been made clearer in certain respects.

Article 13: Right of access

This Article reproduces point (a) of Article 12 of the Directive.

A change has been made regarding the expenses a person exercising his right of access may be required to reimburse. Article 12 provides that such expenses may not be excessive. It is proposed here, by contrast, that the service should be provided entirely free of charge.

It is also proposed that no use be made of the option in the Directive of limiting to automated decisions the obligation for the controller to inform data subjects of knowledge of the logic involved in any automatic processing of data.

Article 14: Rectification

This Article is, like Articles 15 and 16, devoted to one of the three measures which the controller must take where the processing of data does not comply with the Regulation. These three Articles of the present Regulation reproduce point (b) of Article 12 of the Directive, amended slightly in the interests of clarity.

Article 15: Blocking

This Article describes in some detail situations where:

- this technical operation should be carried out: contesting of the accuracy of processed data in relation to the objective pursued, maintenance of data for reasons of proof, and demand by the data subject that data be maintained rather than blocked;

- blocked data may be reused.

Article 16: Erasure

Paragraph 1 prescribes erasure of personal data that have been processed in an unlawful way, in particular because the requirements with regard to data quality, legitimate processing and sensitive data have been violated.

Paragraph 2 repeats the principle that personal data shall only be kept as long as necessary to achieve the purpose they were collected for.

Article 17: Notification to third parties

This Article reproduces point (c) of Article 12 of the Directive.

Section VI: Exemptions and restrictions

Article 18: Exemptions and restrictions

This Article partially reproduces Article 13 of the Directive, which leaves Member States certain options which, if exercised, must nevertheless satisfy certain conditions:

- as regards data subjects' rights and controllers' obligations the scope of which may be restricted: unlike Article 13 of the Directive, the present Article derogates from the giving of information to data subjects (Articles 11 and 12) and from their right of access (Article 13). The conditions under which the quality of data may be derogated from, in so far as the purpose of the processing is compatible, have already been dealt with under Article 6 of this Regulation on change of purpose. And it is inappropriate to include in Article 18 of this Regulation a reference to Articles 14 to16. Exercise of the rights provided for in those Articles presupposes that the right of access has been granted; without access they cannot function; if access is granted, the exemption from these rights is no longer justified.

- as regards the grounds on which data subjects' rights may be restricted: the grounds of national security, defence and public security listed in points (a), (b) and (c) of Article 13(1) have not been reproduced as they do not apply to Community institutions and bodies.

- as regards the safeguards that must be introduced: Article 13 of the Directive does not authorise an outright derogation, but merely exemptions and restrictions implemented on a case-by-case basis. The purpose of paragraphs 3 and 4 of this Article is therefore to provide various safeguards with a view to protecting data subjects who are denied access in a particular case: right to be informed of the main reasons why access has been denied and of the possibility of having recourse to the supervisory authority, right to be informed *ex post facto*.

Section VII: The data subject's right to object

Article 19: The data subject's right to object

This Article reproduces point (a) of Article 14 of the Directive, which gives Member States a degree of discretion over the scope of this right. Some clarification is therefore needed in the present Regulation.

Point (b) of Article 14 on the right to object to direct marketing does not concern the activities of Community institutions and bodies.

Similarly, with regard to the scope of the right to object as defined in point (a) of Article 14 of the Directive, it should be pointed out that the reference to processing carried out under Article 7(f) of the Directive - to which Article 14(a) of the Directive refers - cannot apply to Community institutions and bodies because, as already indicated, Article 7(f) is itself not applicable in this specific Community context.

Article 20: The data subject's right to lodge complaints

The right to lodge complaints is the logical counterpart of the power of the European Data Protection Supervisor to hear claims in conformity with Article 28(4) of the Directive.

Article 21: Automated individual decisions

This Article reproduces Article 15 of the Directive.

Some of the examples given in Article 15(1) of the Directive concerning the evaluation of certain personal aspects (notably creditworthiness) would be out of place in the specific context of the Regulation and have not been reproduced.

Section VIII: Confidentiality and security of processing

Article 22: Confidentiality of processing

This Article reproduces Article 16 of the Directive.

It has not been considered necessary to reproduce the derogation possibility provided for in the Directive concerning legal obligations as it would duplicate Article 6 on change of purpose.

Article 23: Security of processing

This Article reproduces Article 17(1) of the Directive, while making it clearer.

Paragraph 1 of the present Article reproduces the second subparagraph of Article 17(1).

Paragraph 2 is devoted to the security measures to be taken in the case of manually processed data.

Paragraph 3 clarifies the first subparagraph of Article 17, the wording of which is very general. It is based on various recent Council of Europe recommendations on data protection and on the Convention for implementing the Schengen Agreement (Article 118).

It is clear that, in practice, the security measures to be taken will have to fit into the wider pattern of measures which the institutions and bodies have already taken with regard to the security of information systems (see, for example, the Commission Decision of 23 November 1995 which seeks to protect the integrity, availability and confidentiality of information systems).

Article 24: Processing of personal data on behalf of controllers

This Article reproduces paragraphs 2 to 4 of Article 17 of the Directive.

Section IX: Data protection officer

Article 25: Data protection officer

This Article stipulates that each institution and body will have to appoint a data protection officer responsible for ensuring in an independent manner that data are protected within the institution or body in question.

The appointment of data protection officers is provided for in Article 18(2) of the Directive as an option Member States may make use of. According to that Article, such an appointment makes it possible to simplify, or even grant exemption from, the obligation to notify processing operations to the supervisory authority.

The Directive is influenced in this respect by a practice which is well established in some Member States and which makes it possible to protect people effectively.

A few comments are in order concerning the officer's appointment, the duties he/she is to perform, the safeguards that are to be introduced in order to enable him/her to perform those duties, and his/her relationship with the supervisory authority.

- Appointment of the data protection officer: each institution and body will be required to appoint at least one officer. Some institutions - such as the Commission - will probably find it necessary to appoint several officers owing to the scale of personal data processing within the institution.

- The officer's duties: his/her main duty is laid down in paragraph 1 of this Article. The wording is based closely on the Directive: he/she must ensure the internal application of data protection and keep a register of all processing operations carried out by the institution or body. Stress is placed in this Article on the officer's role of informing data subjects and controllers about their rights and obligations in the data protection field. The provision of such information is the main prerequisite for proper application of the protection afforded by the Directive. Stress has therefore been placed on this aspect in the first indent of paragraph 1, although substantively it adds nothing to the Directive's more general wording. A number of more specific tasks are also entrusted to the officer to help him/her perform his/her duties: he/she can make proposals aimed at improving data protection within the institution or body, and he/she can be consulted by the authority that appointed him/her, by controllers or by the staff committee. In addition the data protection officer is under an obligation to cooperate with the European Data Protection Supervisor (second indent). The obligation laid down in the fifth indent serves to facilitate the identification of processing operations, which present specific risks, by means of prior checking by the EDPS.

- Safeguards to enable the officer to perform his/her duties: the safeguards that are laid down are all intended to underpin as far as possible the key feature of the officer's role as reproduced from the Directive, namely his/her independence.

Articles 26 and 27: Registration with the data protection officer

In the interests of openness, Article 27 provides, in accordance with the wording of the Directive, that the officer will have to keep a register of processing operations carried out within the institution or body.

To help him/her do so, controllers may notify the officer of such processing operations before they are carried out.

A list of information to be furnished to the officer is reproduced from Article 19(1) of the Directive, to which Article 21(2) of the Directive refers.

The list contained in the Directive is a minimum list. In the interests of greater openness regarding processing operations carried out by institutions and bodies, it is proposed that there be added to this list information on the legal basis of the processing (e.g. the provisions of Community law which make the processing necessary)and the length of time the data will be kept It should be noted once more that representation of the controller as referred to in Article 19(1)(a) of the Directive does not apply in the case of Community institutions and bodies.

Section X: Prior checking by the European Data Protection Officer

Article 28: Prior checking by the European Data Protection Officer

This Article is equivalent to Article 20 of the Directive.

The Directive provides for selective checking of the lawfulness of processing operations according to the risks they may present to data subjects' rights:

- the notification of processing operations to the supervisory authority can as a rule be simplified, or even waived, under certain conditions, notably where a data protection officer has been appointed.

- notification remains necessary, and must even take the enhanced form of a prior check, in the case of processing operations presenting specific risks.

The present Regulation draws the necessary conclusions from the attachment of a data protection officer to Community institutions and bodies by limiting the obligation to notify the Community supervisory authority to processing operations presenting specific risks.

Using an option left by Article 20(2) of the Directive, processing operations presenting a risk will have to be notified to the supervisory authority by the data protection officer of each institution or body.

Article 20(1) of the Directive stipulates that it is for Member States to determine the processing operations likely to present specific risks. Recital 53 states that these risks may, if Member States so wish, be specified in national legislation, leaving open the possibility for supervisory authorities also to form their own view of the concept of processing operations presenting specific risks. The present Article takes the latter course and empowers the supervisory authority to determine which processing operations present specific risks. Several examples, based on recital 53, are, however, given in the Article itself.

Based on recital 54, paragraph 3 of the present Article provides that the supervisory authority in receipt of a notification of a processing operation presenting specific risks must deliver an opinion on the lawfulness of the processing operation envisaged. It will be for the institution or body which notified the processing operation to draw the necessary operational consequences from it.

Chapter III: Judicial Remedies and Sanctions

Articles 29 and 30

These Articles transpose Articles 22, 23 and 24 of the Directive. In a Community governed by the rule of law, it must be possible for the rights conferred on individuals to be exercised also where those rights are violated by a Community institution or body. In accordance with the provisions of the Treaty concerning the Community's non-contractual liability, the Community must make good any damage caused by its institutions or by its servants in the performance of their duties, and the Court of Justice has jurisdiction in disputes relating to compensation for such damage.

Chapter IV: Protection of personal data and privacy in the context of internal telecommunications networks.

This section reproduces the provisions of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector as far as they are fitted for application to the Community institutions and bodies. Most provisions had to be adapted to the specific circumstances within the Community institutions and bodies.

Article 31: Scope

The scope of this chapter is limited to those telecommunication networks which are operated under the control of the Community institutions and bodies. Articles 31 to 37 thus only apply if the Community institutions and bodies are indeed in a position to determine the conditions of operation of the telecommunication networks concerned.

Article 32: Security

This provision reproduces Article 4 of Directive 97/66/EC.

In case a telecommunication network or line has a connection to a publicly available network or in case such a network or line is hired from or operated in cooperation with a provider of a publicly available network it might be necessary for the Community institution or body to cooperate with the network or service provider involved in order to guarantee a sufficient level of security.

Article 33: Confidentiality

This provision reproduces Article 5 of Directive 97/66/EC.

In the interest of the purposes mentioned in Article 34 it might be necessary to monitor in particular cases the use of a particular telecommunication network. Examples are the storage of certain data in relation to telephone calls for billing purposes or the surveillance of the use of the internet facilities offered to officials of the Community institutions and bodies. In line with the general principles of this Regulation the degree of such interception or surveillance should remain as limited as possible.

Article 34: Traffic and billing data

This provision reproduces Article 6 of Directive 97/66/EC.

Article 34 specifies the limits of processing personal data for billing, budgetary and traffic management purposes.

Article 35: Directories of users

This provision reproduces Article 11 of Directive 97/66/EC.

Because it is necessary for the proper functioning of the Community institutions and bodies, users, i.e. normally officials, have not been granted the right to be omitted from directories. However their personal data contained in such directories shall be limited to what is necessary to for the specific purposes of the directory. This implies that with regard to particular data the official shall have a choice whether or not he or she wants these data to be included. An example is the right to require that not all official first names received by birth are mentioned in a directory, but only the first name by which an official is known to its colleagues, provided of course that it is not a pseudonym.

Article 36: Identification of calling and connected line identification.

This provision reproduces Article 8 of Directive 97/66/EC. However Article 8(3) of this Directive is not repeated here because it is considered that the rejection of incoming calls from colleagues is not an appropriate means within the context of the Community institutions and bodies.

Article 37: Exceptions

This provision reproduces Article 9 of Directive 97/66/EC.

Chapter V: Supervisory Authority: European Data Protection Supervisor

Articles 38-47

The supervisory authority has been modelled, *mutatis mutandis*, on Article 28 of the Directive, which affords clear guidance on the independence of supervisory authorities set up at national level and on the powers they may exercise. Inasmuch as the above-mentioned provision creates obligations on the part of Member States, Article 286 of the Treaty requires that the same obligations be "transposed" to Community institutions and bodies.

Article 39: Appointment of the EDPS

As regards the procedure for appointing the supervisory authority, the solution adopted is based on the provisions concerning the European Ombudsman (Article 195 of the Treaty). In the opinion of the Advisory Group on Data Protection set up by Article 29 of the Directive, appointment of the authority by the European Parliament is the appropriate method. However contrary to the appointment of the European Ombudsman consultation of the Commission and the Council by the European Parliament has been made obligatory.

Article 46: Powers of the EDPS

The power to intervene in proceedings before the Court of Justice and the Court of First Instance as laid down in Article 46(2)(e) 'transposes' Article 28(3), 3rd indent, of the Directive.

Article 46(7) transposes the last paragraph of Article 28(1) of the Directive. An amendment of the Rules of Procedure of the Court of Justice and Court of First Instance will be necessary to enable them to deal with actions brought against the EDPS.

Final Provisions

Article 48

This provision reproduces Article 32(2) of the Directive by granting a transitional period for compliance with the Regulation for processing already under way. Instead of a three-year period a one-year period is proposed.

FINANCIAL STATEMENT

1. TITLE OF OPERATION

Proposal for a Regulation of the European Parliament and of the Council on protection of individuals with regard to the processing of personal data by the institutions and bodies of the European Community and on the free movement on such data.

2. BUDGET HEADING INVOLVED

New Chapter 39 (to be created) of Section 1 (EP), Title 3 of the General Budget.

3. LEGAL BASIS

Article 286 of the Treaty establishing the European Community (as inserted by the Amsterdam Treaty).

Article 286

1. *From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.*

2. *Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 189b, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate."*

4. DESCRIPTION OF OPERATION

4.1 General objective

1. The establishment of an independent supervisory body as required by the new Article 286(2) of the EC Treaty (the European Data Protection Supervisor, EDPS, see Annex I) responsible for monitoring the application of data protection rules and principles within the Community institutions and bodies.

2. The appointment of one or more Data Protection Officers (DPO) in each Community institution and body (see Annexes IIa and IIb).

4.2 Period covered and arrangements for renewal

These structures will be permanent.

5. CLASSIFICATION OF EXPENDITURE OR REVENUE

5.1 Non-compulsory expenditure

5.2 Non-differentiated appropriations

5.3 Type of revenue involved

N/A

6. TYPE OF EXPENDITURE OR REVENUE

Administrative expenditure.

7. FINANCIAL IMPACT

See paragraph 10.

8. FRAUD PREVENTION MEASURES

The rules and procedures governing procurement of goods and services for the Communities will be strictly complied with, in accordance with the financial regulation applicable to the general budget of the European Communities, the regulation on modalities for the implementation of the financial regulation and internal rules.

The relevant protective clauses will be included in all agreements and contracts between the European Data Protection Supervisor or other Community bodies or institutions and contractors.

Control measures will be systematically included in all contracts and agreements, such as periodic reporting and evaluation of predetermined deliverables at predetermined contract milestones. Verification of effective performance will be made before any payments are authorised.

9. ELEMENTS OF COST-EFFECTIVENESS ANALYSIS

9.1 Specific and quantified objectives; target population

- Specific objectives:

To ensure the introduction, application and monitoring of data protection rules in the Community institutions and bodies (an obligation under the new Article 286 of the EC Treaty).

- Target population:

All natural persons whose personal data is processed by Community institutions and bodies. The rules laid down in the Regulation will be of benefit to the Community in general, the employees in the Community institutions and bodies, citizens and contractors to the Community who may be affected by the level of data protection in the Community institutions and bodies.

9.2 Grounds for the operation

Being established on the basis of the new Article 286 of the EC Treaty, the EDPS will be a Community body, and therefore it will be financed by the Community budget.

- Choice of ways and means

* advantages over possible alternatives:

EDPS

The new Article 286 of the EC Treaty requires the establishment of the EDPS, which will not be part of the Commission but constitutes a new independent Community body, performing its tasks on an inter institutional level, i.e. monitoring all other Community institutions and bodies. The Commission has estimated both the number of officials that need to be employed (see 10.1) and the financial impact.(see 10.2) The only point of reference the Commission had when establishing the figures was the national data protection authorities. However they are not entirely comparable with the EDPS. Unlike the EDPS they in general monitor both the public and private sector. In addition there are far less Community institutions and bodies than national public authorities. This comparison makes it clear that there are good arguments to employ fewer officials in the EDPS's office than in the national authorities. On the other hand the amount of work caused by some of the tasks of the EDPS does not depend on the size of the institutions or bodies concerned or the number of processing operations they carry out.

DPO

The proposal for a Regulation foresees that all Community institutions and bodies appoint at least one DPO.

As far as other institutions and bodies than the Commission are concerned, they have been consulted, and their estimates have been included in this financial sheet. The Secretariat General of the EP has indicated that it is up to each institution and body itself to estimate its needs and that it will not express its opinion on the estimates.

As far as the Commission services are concerned, it is expected that they appoint one part time DPO for each Commission service from existing resources, rather than to appoint one or more full time DPOs for the Commission as a whole. The figures in this financial statement are based on this assumption.

There are various reasons to assign to each Commission service its own DPO. The Commission services constitute separate organisational entities. The nature of the data processing operations may vary widely in each Commission service. A DPO needs to possess a detailed knowledge of what is happening in the area of data protection in the service he or she is responsible for. Within one of the Commission services (DG XV) a successful pilot project has been conducted on these lines. After the entry into force of the Regulation experience may show that some services need more DPO time and others less.

Services would appoint as DPOs members of their existing staff, who would need to spend only a small part of their working time (estimated at 5% on average) on their tasks as DPO. It is foreseen in addition that the DPO in the Secretariat General should be responsible for coordinating the work of all the Commission DPOs. In view of these additional coordinating tasks, this 'central' DPO will need to spend more than 5% of his/her working time on the assigned tasks, perhaps as much as 25%. In addition a few other services have clearly indicated that they will need slightly more than 5% (we have estimated the needs of these services at 10% instead of 5%).

External data protection experts

The Commission further recommends that, at least in the initial phase, the DPOs should be supported and advised by external data protection experts. Contrary to the model used by DG XV, where the DPO is assisted by his 'own' external expert, the financial statement is based on three full time external advisers for the Commission as a whole.

* explanatory reference to similar Community or national operations

The idea of infrastructural support of the EDPS by the organisation of the European Parliament is based on the organisation of the European Ombudsman.

Concerning the DPOs, DG XV's experience as well as national practice have served as an example.

* spin-off and multiplier effects expected

None. This has been discussed with the Informatics Directorate. The software and know-how is already present today, and so no extra expense is expected.

- Main factors of uncertainty which could affect the specific results of the operation

  The financial statement is based on the assumption that the EDPS will be provided with the necessary infrastructural support by the European Parliament (see Annex I).

9.3 Monitoring and evaluation of the operation

- Performance indicators selected

  * output indicators (measuring activities used)

  The EDPS will produce an Annual Report. The level of activity of the EDPS will, among other things (See Article 47 of the proposal for a Regulation), be seen in 1) the number of complaints received or taken up on own initiative, 2) the number of decisions taken, 3) the number of audits carried out.

  Concerning DPO: Activity reports.

  * impact indicators (measuring performance against objectives)

  1. Complaints decided against the Community institutions and bodies.

  2. The level of compliance estimated on the basis of the audits performed.

- Details and frequency of planned evaluations

  Evaluations should be based on the Annual Reports. The 'central' DPO will coordinate the work of the DPOs and in addition the EDPS will monitor their work and advise on the correct application of rules.

10. ADMINISTRATIVE EXPENDITURE (SECTION III, PART A OF THE BUDGET)

The actual mobilisation of the necessary administrative resources will depend on the annual decisions taken by the respective institutions or bodies on the allocation of resources taking into account the number of staff and amounts authorised by the budgetary authority.

As far as the estimations by the Commission of the effects of establishment of the EDPS are concerned, they are an indicative and preliminary nature. They do not prejudge the costs, which the European parliament may estimate, taking into account that the Secretariat General of the European Parliament has informed the Commission services that it is for each institution to estimate its needs itself and that it does not wish to express itself on the estimations made by the Commission.

10.1 Effect on the number of posts

Type of post	Staff to be assigned to managing the operation		Source		Duration
	Permanent posts	Temporary posts	Existing resources in the DG or bodies concerned	Additional resources	

EDPS (see Annex I)

Officials or temporary staff	A	6	-	-	6	Unlimited.
	B	2	-	-	2	-
	C	2	-	-	2	-
	D	-	-	-	-	-
Other resources		-	-	-	-	-
		-	-	-	-	-
Total		10	-	-	10	-

DPO Commission (see Annex IIb)

Officials or temporary staff	A	2.40	-	2.40		Unlimited
	B	-	-	-	-	-
	C	-	-	-	-	-
	D	-	-	-	-	-
Other resources (A07002 technical assistance)		3	-	3	-	-
Total		5.40	-	5.40		-

DPO other institutions and bodies (see Annex IIc)

Officials or temporary staff	A	17	-	17	-	Unlimited
	B	-	-	-	-	-
	C	-	-	-	-	-
	D	-	-	-	-	-
Other resources (A07002 technical assistance)		2	-	2	-	-
Total		19	-	19	-	-

GRAND TOTAL

Type of post		Staff to be assigned to managing the operation		Source		Duration
		Permanent posts	Temporary posts	Existing resources in the DG or bodies concerned	Additional resources	
Officials or temporary staff	A	25.40	-	19.40	6	Unlimited
	B	2	-	-	2	-
	C	2	-	-	2	-
	D	-	-	-	-	-
Other resources		5	-	5	-	-
Total		34.40	-	24.40	10	-

10.2 Overall financial impact of additional human resources

The estimation of the financial impact is carried out on the basis of the average cost of an official of the Commission in Brussels (Grade A-1, A-2, A-4, A-5 and A-7).

EDPS

	Amounts	Method of calculation
Officials	1 080 000	10 officials x EUR 108 000 (see Annex I)
Temporary staff		
Other resources		
1 080 000		

DPO Commission

	Amounts	Method of calculation
Officials	432 000	2.40 officials x EUR 108 000 (see Annex IIb)
Temporary staff		
Other resources	339 000	3 contracts x EUR 113 000. (A-7002 technical assistance)(see Annex IIb)
	771 000	

DPO other institutions and bodies

	Amounts	Method of calculation
Officials	1 836 000	17 officials x EUR 108 000 (see Annex IIc)
Temporary staff		
Other resources	220 000	16 contracts x EUR 13 750 (see Annex IIc)
	2 056 000	

GRAND TOTAL

	Amounts	Method of calculation
Officials	3 348 000	See above
Temporary staff		
Other resources	559 000	
	3 907 000	

10.3 Increase in other administrative expenditure as a result of the operation

The incidence of other potential costs for the EDPS depends on the extent to which the EDPS can be integrated in the existing infrastructure of the European Parliament (see Annex I). The estimate of the financial consequences for the European Parliament (EP) of the proposal to integrate the office of the EDPS administratively in the organisation of the EP remains to be confirmed by the EP.

Annex I

Office of the European Data Protection Supervisor

The figures on the office of the EDPS are based on the assumption that the following services can be obtained by integrating the EDPS's office into the existing infrastructure of the European Parliament in a similar way to the European Ombudsman.

- Translation
- Interpretation
- Administrative functions such as: Administration of missions, professional training, personnel (recruitment, medical exams, pay, social matters, career matters etc.), property matters, office automation, equipment and computing development, mail services, communications, transport, furniture, photocopiers, office supplies, usher services, drivers, removers, meeting facilities

- Communication: Telephones and faxes, electronic documentation transfer systems. PCs and printers, database access

- Security

- External offices

- Press and PR.

- Publishing: Annual report, distribution of documentation, printing.

- Purchasing of publications and subscription to periodicals.

The probable total staff will amount to:

A grade: 6

B grade: 2

C grade: 2

Total: 10

Annex IIa

Data Protection Officer

The officials who will be appointed as DPOs will only spend part of their working time on carrying out their tasks as a DPO (estimated between 5% and 10% on an average, see 9.2.). They can seek the assistance of external data protection experts, who can support and advice them.

The tasks and responsibilities assigned to the DPO are listed below. The DPO will be able to draw advice from the external data protection experts with regard to all these issues.

Data protection officers will be responsible for:

- ensuring that controllers and data subjects are informed about their rights and obligations;

- cooperating with the European Data Protection Supervisor at the latter's request or on his/her own initiative;

- ensuring in an independent manner the internal application of provisions of the Regulation and of all other provisions adopted to implement these rules;

- keeping the register of processing operations carried out by the controller;

- making recommendations for the practical improvement of data protection;

- advising the Community institution or body, which appointed him/her and the controller, concerned on matters concerning the application of data protection provisions;

- investigating, on his/her own initiative or at the request of the Community institution or body which appointed him/her, the controller, the Staff Committee concerned or the data subject, matters and occurrences directly relating to his/her tasks and come to his/her notice;

- consultation by the Community institution or body which appointed him/her, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation.

The DPO needs - at least initially- to be able to draw on independent advice by external experts in the field of data protection. These external experts will provide advice, as and when the DPO may require, on the legal, organisational and technical aspects of personal data protection, so as to assist the DPO in all of his tasks.

More in particular the external experts could provide advice with regard to:

- the maintaining of the register of processing operations which contain personal data;

- assessing the risks that these processing operations present for the privacy of the individuals concerned; and

- countering such risks, bearing in mind the need to contribute to the development of straight forward guidelines for best practice which can in due course be applicable by other Commission services.

The main areas in which the expert's advice and experience will probably be necessary in this respect are:

(a) requisite data quality;

(b) exercise of the rights of the data subjects;

(c) new information systems;

(d) external processors and outsourcing;

(e) familiarisation and training of staff;

(f) preparation of guidelines;

(g) confidentiality and security measures;

(h) activities report.

Annex IIb

Data Protection Officers in the Commission services

- Secretariat-General
- Task Force Justice and Home Affairs
- OLAF
- Inspectorate-General
- Legal Service
- Spokesman's Service
- Joint Interpreting and Conference Service
- Statistical Office
- Translation Service
- Informatics Directorate
- DG I - External Relations: Commercial Policy and Relations with North America, the Far East, Australia and New Zealand
- DG IA - External Relations: Europe and the New Independent States, Common Foreign and Security Policy and External Missions
- DG IB - External Relations: Southern Mediterranean, TOP and Near East, Latin America, South and South-East Asia and North-South Cooperation
- DG II - Economic and Financial Affairs
- DG III - Industry
- DG IV - Competition
- DG V - Employment, Industrial Relations and Social Affairs
- DG VI - Agriculture
- DG VII - Transport
- DG VIII - Development
- DG IX - Personnel and Administration
- DG X - Information, Communication, Culture, Audio-visual Media
- DG XI - Environment, Nuclear Safety and Civil Protection

- DG XII - Science, Research and Development Joint Research Centre
- DG XIII - Telecommunications, Information Market and Exploitation of Research
- DG XIV - Fisheries
- DG XV - Internal Market and Financial Services
- DG XVI - Regional Policies and Cohesion
- DG XVII - Energy
- DG XIX - Budgets
- DG XX - Financial Control
- DG XXI - Taxation and Customs Union
- DG XXII - Education, Training and Youth
- DG XXIII - Enterprise Policy, Distributive Trades, Tourism and Cooperatives
- DG XXIV - Consumer Policy and Consumer Health Protection
- European Community Humanitarian Office (ECHO)
- Task Force for the Accession Negotiations (TFAN)
- Euratom Supply Agency
- Office for Official Publications of the European Communities
- Relex Common Service (SCR)

Total number = 40

As explained under paragraph 9.2. it is foreseen that each Commission service will appoint its own DPO of its existing staff, rather than to appoint one or more DPOs for the Commission as a whole. The figures in this financial statement are based on this assumption. On average 5% of a full time official is considered necessary for each service. Some services will need more, others less. A number of services have already indicated they need more than 5%, and their needs have been estimated at 10%. These figures add up to 2.40 full time officials for the whole Commission. It is foreseen in addition that the DPO in the Secretariat-General should be responsible for coordinating the work of all the Commission DPOs. In view of these additional task he or she will spend more than 5% of his working time on the assigned tasks, perhaps as much as 25%.This is already included in the estimation of 2.40 officials..

Further it is foreseen, at least in the initial phase, to establish contracts with external experts (three full-time experts for the whole Commission).

Annex IIc

Data Protection Officers in the Institutions and bodies outside the Commission

European Parliament	2.0
European Ombudsman	1.0
Council of the European Union	2.0
Court of Justice	1.0
Court of Auditors	1.0
European Investment Bank	1.0
Economic and Social Committee	1.0
Committee of the Regions	1.0
European Central Bank	1.0
CEDEFOP - European Centre for the Development of Vocational Training	0.5
European Foundation for the Improvement of Living and Working Conditions	0.5
European Environment Agency	0.5
European Training Foundation	0.5
European Monitoring Centre for Drugs and Drug Addiction	0.5
European Agency for the Evaluation of Medicinal Products	0.5
Office of Harmonisation in the Internal Market (Trade Marks and Designs)	0.5
European Agency for Safety and Health at Work	0.5
Community Plant Variety Office	0.5
Translation Centre for the bodies of the Union	1.0
European Observatory for Racism and Xenophobia	0.5

Total number = 17 (full-time officials x EUR 108 000)

Apart from the DPOs attached to the institutions and bodies listed above also contracts with external data protection experts are envisaged. On an average 22 working days a year have been estimated for each institution or body. This number is comparable to the number of days available per Commission service. The average cost per service of such contracts is estimated at EUR 13 750 a year.

ISSN 0254-1475

COM(1999) 337 final

DOCUMENTS

EN **10 02 06 15**

Catalogue number : CB-CO-99-380-EN-C

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