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

(1999/C 376 E/04)

(Text with EEA relevance)

COM(1999) 337 final — 1999/0153(COD)

(Submitted by the Commission on 17 September 1999)

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,

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

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

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 fully-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.

(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 [1] 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 [2] particularises 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 particularise 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.

---

[1] OJ L 281, 23.11.1995, p. 31.

[2] 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 particularise 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 [1], 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:

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;

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

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

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

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 to 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 of processing

Article 22

Confidentiality and security 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.

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.
