Publicat în Jurnalul Oficial L nr. 8 din 12-01-2001

Abrogat(ă) de Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018

Regulation (EC) No 45/2001 of the European Parliament and of the Council

of 18 December 2000

on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies 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 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 data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies.

(6) 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 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) has been consulted.

(7) The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies.

(8) The principles of data protection should 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 to be reasonably 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.

(9) Directive 95/46/EC 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.

(10) 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) specifies and adds to Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector.

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

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

(13) 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.

(14) To this end measures should be adopted which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

(15) Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union. Access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 of the EC Treaty the scope of which includes Titles V and VI of the Treaty on European Union.

(16) The measures should not apply to bodies established outside the Community framework, nor should the European Data Protection Supervisor be competent to monitor the processing of personal data by such bodies.

(17) The effectiveness of the protection of individuals with regard to the processing of personal data in the Union presupposes the consistency of the relevant rules and procedures applicable to activities pertaining to different legal contexts. The development of fundamental principles on the protection of personal data in the fields of judicial cooperation in criminal affairs and police and customs cooperation, and the setting-up of a secretariat for the joint supervisory authorities established by the Europol Convention, the Convention on the Use of Information Technology for Customs Purposes and the Schengen Convention represent a first step in this regard.

(18) This Regulation should not affect the rights and obligations of Member States under Directives 95/46/EC and 97/66/EC. It is not intended to change existing procedures and practices lawfully implemented by the Member States in the field of national security, prevention of disorder or prevention, detection, investigation and prosecution of criminal offences in compliance with the Protocol on Privileges and Immunities of the European Communities and with international law.

(19) The Community institutions and bodies should inform the competent authorities in the Member States when they consider that communications on their telecommunications networks should be intercepted, in keeping with the national provisions applicable.

(20) The provisions applicable to the Community institutions and bodies should correspond to those 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 specify and add to those provisions when it comes to ensuring protection in the case of the processing of personal data by the Community institutions and bodies.

(21) 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 authority responsible for ensuring that this Regulation is properly applied.

(22) The rights accorded the data subject and the exercise thereof should not affect the obligations placed on the controller.

(23) The independent supervisory authority should exercise its supervisory functions in accordance with the Treaty and in compliance with human rights and fundamental freedoms. It should conduct its enquiries in compliance with the Protocol on Privileges and Immunities and with the Staff Regulations of Officials of the European Communities and the conditions of employment applicable to Other Servants of the Communities.

(24) The necessary technical measures should be adopted to allow access to the registers of processing operations carried out by Data Protection Officers through the independent supervisory authority.

(25) The decisions of the independent supervisory authority regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the independent supervisory authority may publish reports on specific subjects.

(26) Certain processing operations likely to present specific risks with respect to the rights and freedoms of data subjects are subject to prior checking by the independent supervisory authority. The opinion given in the context of such prior checking, including the opinion resulting from failure to reply within the set period, should be without prejudice to the subsequent exercise by the independent supervisory authority of its powers with regard to the processing operation in question.

(27) Processing of personal data for the performance of 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.

(28) In certain cases the processing of data should be authorised by Community provisions or by acts transposing Community provisions. Nevertheless, in the transitional period during which such provisions do not exist, pending their adoption, the European Data Protection Supervisor may authorise processing of such data provided that adequate safeguards are adopted. In so doing, he should take account in particular of the provisions adopted by the Member States to deal with similar cases.

(29) These cases concern the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life which are necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law or for reasons of substantial public interest. They also concern the processing of data relating to offences, criminal convictions or security measures and authorisation to apply a decision to the data subject which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her.

(30) 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.

(31) Liability arising from any breach of this Regulation is governed by the second paragraph of Article 288 of the Treaty.

(32) In each Community institution or body one or more Data Protection Officers should ensure that the provisions of this Regulation are applied and should advise controllers on fulfilling their obligations.

(33) 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.

(34) Under Article 8(8) of Council Regulation (EC) No 2533/98 of 23 November 1998 concerning the collection of statistical information by the European Central Bank(7), that Regulation is to apply without prejudice to Directive 95 /46/EC.

(35) Under Article 1(2) of Council Regulation (Euratom, EEC) No 1588/90 of 11 June 1990 on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities(8), that Regulation does not derogate from the special Community or national provisions concerning the safeguarding of confidentiality other than statistical confidentiality.

(36) This Regulation does not aim to limit Member States' room for manoeuvre in drawing up their national laws on data protection under Article 32 of Directive 95/46/EC, in accordance with Article 249 of the Treaty,

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 and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC.

2. The independent supervisory authority established by this Regulation, hereinafter referred to as the 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 hereinafter referred to as "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 or her physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" hereinafter referred to as "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" hereinafter referred to as "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 a 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 or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

Article 3

Scope

1. This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

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

Data quality

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 incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual;

(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 that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes.

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 the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof 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 or her consent, or

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

Article 6

Change of purpose

Without prejudice to Articles 4, 5 and 10:

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 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 prevention, investigation, detection and prosecution of serious criminal offences.

Article 7

Transfer of personal data within or between Community institutions or bodies

Without prejudice to Articles 4, 5, 6 and 10:

1. Personal data shall only be transferred 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. Where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer.

The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient.

The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.

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

Article 8

Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC

Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC,

(a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or

(b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

Article 9

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

1. Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to 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 transferred solely to allow tasks covered by the competence of the controller to be carried out.

2. The adequacy of the level of protection afforded by the third 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 recipient third country or recipient international organisation, the rules of law,

both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third 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 third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2.

4. The Commission shall inform the Member States of any cases as referred to in paragraph 3.

5. The Community institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 25(4) and (6) of Directive 95/46/EC, that a third country or an international organisation ensures or does not ensure an adequate level of protection.

6. By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if:

(a) the data subject has given his or 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 entered into 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 a legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case.

7. Without prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

8. The Community institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where they have applied paragraphs 6 and 7.

SECTION 3

SPECIAL CATEGORIES OF PROCESSING

Article 10

The processing of special categories of data

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

2. Paragraph 1 shall not apply where:

(a) the data subject has given his or her express 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 or her consent, or

(b) processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof, or, if necessary, insofar as it is agreed upon by the European Data Protection Supervisor, subject to 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 or 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 safeguards 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, 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 appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, 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 the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards.

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

SECTION 4

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 11

Information to be supplied where the data have been obtained from the data subject

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

(a) the identity of the controller;

(b) the purposes of the processing operation 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 or her;

(f) any further information such as:

(i) the legal basis of the processing operation for which the data are intended,

(ii) the time-limits for storing the data,

(iii) the right to have recourse at any time to the European Data Protection Supervisor,

insofar 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, except for the information referred to in paragraph 1(a), (b) and (d), may be deferred as long as this is necessary for statistical purposes. The information must be provided as soon as the reason for which the information is withheld ceases to exist.

Article 12

Information to be supplied 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 shall 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 or she already has it:

(a) the identity of the controller;

(b) the purposes of the processing operation;

(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 or her;

(f) any further information such as:

(i) the legal basis of the processing operation for which the data are intended,

(ii) the time-limits for storing the data,

(iii) the right to have recourse at any time to the European Data Protection Supervisor,

(iv) the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy,

insofar 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 after consulting the European Data Protection Supervisor.

SECTION 5

RIGHTS OF THE DATA SUBJECT

Article 13

Right of access

The data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller:

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

(b) information at least as to the purposes of the processing operation, the categories of data concerned, and 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 or her.

Article 14

Rectification

The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

Article 15

Blocking

1. The data subject shall have the right to obtain from the controller the blocking of data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data, or;

(b) the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or;

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

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 may not be used.

3. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of a third party.

4. The data subject who requested and obtained the blocking of his or her data shall be informed by the controller before the data are unblocked.

Article 16

Erasure

The data subject shall have the right to obtain from the controller the erasure of data if their processing is unlawful, particularly where the provisions of Sections 1, 2 and 3 of Chapter II have been infringed.

Article 17

Notification to third parties

The data subject shall have the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to Articles 13 to 16 unless this proves impossible or involves a disproportionate effort.

Article 18

The data subject's right to object

The data subject shall have the right:

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

(b) to be informed before personal data are disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use.

Article 19

Automated individual decisions

The data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken.

SECTION 6

EXEMPTIONS AND RESTRICTIONS

Article 20

Exemptions and restrictions

1. The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 and Article 37(1) where such 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 Communities, including monetary, budgetary and taxation matters;

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

(d) the national security, public security or defence of the Member States;

(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the 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 compiling 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 particular individuals.

3. If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor.

4. If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

5. Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect.

SECTION 7

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 21

Confidentiality of processing

A person employed with a Community institution or body and any Community institution or body itself acting as processor, with access to personal data, shall not process them except on instructions from the controller, unless required to do so by national or Community law.

Article 22

Security of processing

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

Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of:

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

(b) preventing any unauthorised reading, copying, alteration or removal of storage media;

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

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

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

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

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

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

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

Article 23

Processing of personal data on behalf of controllers

1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures.

2. The carrying out of a processing operation 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 Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

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 22 shall be in writing or in another equivalent form.

SECTION 8

DATA PROTECTION OFFICER

Article 24

Appointment and tasks of the Data Protection Officer

1. Each Community institution and Community body shall appoint at least one person as data protection officer. That person shall have the task of:

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

(b) responding to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, cooperating with the European Data Protection Supervisor at the latter's request or on his or her own initiative;

(c) ensuring in an independent manner the internal application of the provisions of this Regulation;

(d) keeping a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25(2);

(e) notifying the European Data Protection Supervisor of the processing operations likely to present specific risks within the meaning of Article 27.

That person shall thus ensure 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 selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection.

3. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his or her duty as Data Protection Officer and any other official duties, in particular in relation to the application of the provisions of this Regulation.

4. The Data Protection Officer shall be appointed for a term of between two and five years. He or she shall be eligible for reappointment up to a maximum total term of ten years. He or she may be dismissed from the post of Data Protection Officer by the Community institution or body which appointed him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.

5. After his or her appointment the Data Protection Officer shall be registered with the European Data Protection Supervisor by the institution or body which appointed him or her.

6. The Community institution or body which appointed the Data Protection Officer shall provide him or her with the staff and resources necessary to carry out his or her duties.

7. With respect to the performance of his or her duties, the Data Protection Officer may not receive any instructions.

8. Further implementing rules concerning the Data Protection Officer shall be adopted by each Community institution or body in accordance with the provisions in the Annex. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer.

Article 25

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:

(a) the name and address of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subjects and of the data or categories of data relating to them;

(d) the legal basis of the processing operation for which the data are intended;

(e) the recipients or categories of recipient to whom the data might be disclosed;

(f) a general indication of the time limits for blocking and erasure of the different categories of data;

(g) proposed transfers of data to third countries or international organisations;

(h) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 to ensure security of processing.

3. Any change affecting information referred to in paragraph 2 shall be notified promptly to the Data Protection Officer.

Article 26

Register

A register of processing operations notified in accordance with Article 25 shall be kept by each Data Protection Officer.

The registers shall contain at least the information referred to in Article 25(2)(a) to (g). The registers may be inspected by any person directly or indirectly through the European Data Processing Supervisor.

SECTION 9

PRIOR CHECKING BY THE EUROPEAN DATA PROTECTION SUPERVISOR AND OBLIGATION TO COOPERATE

Article 27

Prior checking

1. 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 shall be subject to prior checking by the European Data Protection Supervisor.

2. The following processing operations are likely to present such risks:

(a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;

(b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;

(c) processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;

(d) processing operations for the purpose of excluding individuals from a right, benefit or contract.

3. 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 as to the need for prior checking, shall consult the European Data Protection Supervisor.

4. The European Data Protection Supervisor shall deliver his or her opinion within two months following receipt of the notification. This period may be suspended until the European Data Protection Supervisor has obtained any further information that he or she may have requested. When the complexity of the matter so requires, this period may also be extended for a further two months, by decision of the European Data Protection Supervisor. This decision shall be notified to the controller prior to expiry of the initial two-month period.

If the opinion has not been delivered by the end of the two-month period, or any extension thereof, it shall be deemed to be favourable.

If the opinion of the European Data Protection Supervisor is that the notified processing may involve a breach of any provision of this Regulation, he or she shall where appropriate make proposals to avoid such breach. Where the controller does not modify the processing operation accordingly, the European Data Protection Supervisor may exercise the powers granted to him or her under Article 47(1).

5. The European Data Protection Supervisor shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 2. The register shall contain the information referred to in Article 25 and shall be open to public inspection.

Article 28

Consultation

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

2. When it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.

Article 29

Obligation to provide information

The Community institutions and bodies shall inform the European Data Protection Supervisor of the measures taken further to his or her decisions or authorisations as referred to in Article 46(h).

Article 30

Obligation to cooperate

At his or her request, controllers shall assist the European Data Protection Supervisor in the performance of his or her duties, in particular by providing the information referred to in Article 47(2)(a) and by granting access as provided in Article 47(2)(b).

Article 31

Obligation to react to allegations

In response to the European Data Protection Supervisor's exercise of his or her powers under Article 47(1)(b), the controller concerned shall inform the Supervisor of its views within a reasonable period to be specified by the Supervisor. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.

CHAPTER III

REMEDIES

Article 32

Remedies

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

2. Without prejudice to any judicial remedy, every data subject may lodge a complaint with the European Data Protection Supervisor if he or she considers that his or her rights under Article 286 of the Treaty have been infringed as a result of the processing of his or her personal data by a Community institution or body.

In the absence of a response by the European Data Protection Supervisor within six months, the complaint shall be deemed to have been rejected.

3. Actions against decisions of the European Data Protection Supervisor shall be brought before the Court of Justice of the European Communities.

4. Any person who has suffered damage because of an unlawful processing operation or any action incompatible with this Regulation shall have the right to have the damage made good in accordance with Article 288 of the Treaty.

Article 33

Complaints by Community staff

Any person employed with a Community institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged breach of the provisions of this Regulation governing the processing of personal data, without acting through official channels. No-one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging a breach of the provisions governing the processing of personal data.

CHAPTER IV

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

Article 34

Scope

Without prejudice 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 or terminal equipment operated under the control of a Community institution or body.

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

Article 35

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 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 the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.

Article 36

Confidentiality of communications

Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law.

Article 37

Traffic and billing data

1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are 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.

2. If necessary, traffic data as indicated in a list agreed by the European Data Protection Supervisor may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. These data shall be erased or made anonymous as soon as possible and no later than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court.

3. Processing of traffic and billing data 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 or other records of calls made.

Article 38

Directories of users

1. Personal data contained in printed or electronic directories of users and access to such directories shall be limited to what is strictly 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 39

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 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 40

Derogations

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

INDEPENDENT SUPERVISORY AUTHORITY: THE EUROPEAN DATA PROTECTION SUPERVISOR

Article 41

European Data Protection Supervisor

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

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

Article 42

Appointment

1. The European Parliament and the Council shall appoint by common accord the European Data Protection Supervisor for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates.

An Assistant Supervisor shall be appointed in accordance with the same procedure and for the same term, who shall assist the Supervisor in all the latter's duties and act as a replacement when the Supervisor is absent or prevented from attending to them.

2. The European Data Protection Supervisor shall be chosen from persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities referred to in Article 28 of Directive 95/46/EC.

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

4. Apart from normal replacement or death, the duties of the European Data Protection Supervisor shall end in the event of resignation or compulsory retirement in accordance with paragraph 5.

5. The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.

6. In the event of normal replacement or voluntary resignation, the European Data Protection Supervisor shall nevertheless remain in office until he or she has been replaced.

7. Articles 12 to 15 and 18 of the Protocol on the Privileges and Immunities of the European Communities shall also apply to the European Data Protection Supervisor.

8. Paragraphs 2 to 7 shall apply to the Assistant Supervisor.

Article 43

Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources

1. The European Parliament, the Council and the Commission shall by common accord determine the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties and in particular his or her salary, allowances and any other benefits in lieu of remuneration.

2. The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.

3. The European Data Protection Supervisor's budget shall be shown in a separate budget heading in Section VIII of the general budget of the European Union.

4. The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and the other staff members of the Secretariat 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 or her direction. Their numbers shall be decided each year as part of the budgetary procedure.

5. The officials and the other staff members of the European Data Protection Supervisor's Secretariat shall be subject to the rules and regulations applicable to officials and other servants of the European Communities.

6. In matters concerning the Secretariat 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 44

Independence

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

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

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

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

Article 45

Professional secrecy

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

Article 46

Duties

The European Data Protection Supervisor shall:

(a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;

(b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;

(c) monitor and ensure 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 body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;

C.H.F. Piața Neamț

(d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;

(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(f) (i) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that Directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;

(ii) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;

(g) 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;

(h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);

(i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26;

(j) carry out a prior check of processing notified to him or her;

(k) establish his or her Rules of Procedure.

Article 47

Powers

1. The European Data Protection Supervisor may:

(a) give advice to data subjects in the exercise of their rights;

(b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;

(d) warn or admonish the controller;

(e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;

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

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

(h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;

(i) intervene in actions brought before the Court of Justice of the European Communities.

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

(a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;

(b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

Article 48

Activities report

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

2. The European Data Protection Supervisor shall forward the activities report to the other Community institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament, in particular in relation to the description of the measures taken in response to the remarks made by the European Data Protection Supervisor under Article 31.

CHAPTER VI

FINAL PROVISIONS

Article 49

Sanctions

Any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his or 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 European Communities or in the conditions of employment applicable to other servants.

Article 50

Transitional period

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

Article 51

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, 18 December 2000.

For the European Parliament

The President

N. Fontaine

For the Council

The President

D. Voynet

(1) OJ C 376E, 28.12.1999, p. 24.

(2) OJ C 51, 23.2.2000, p. 48.

(3) Opinion of the European Parliament of 14 November 2000 and Council Decision of 30 November 2000.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 52, 22.2.1997, p. 1.

(7) OJ L 318, 27.11.1998, p. 8.

(8) OJ L 151, 15. 6.1990, p. 1. Regulation as amended by Regulation (EC) No 322/97 (OJ L 52, 22.2.1997, p. 1).

ANNEX

1. The Data Protection Officer may make recommendations for the practical improvement of data protection to the Community institution or body which appointed him or her and advise it and the controller concerned on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the Community institution or body which appointed him or her, the controller, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller.

2. The Data Protection Officer may be consulted by the Community institution or body which appointed him or 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 this Regulation.

3. No one shall suffer prejudice on account of a matter brought to the attention of the competent Data Protection Officer alleging that a breach of the provisions of this Regulation has taken place.

4. Every controller concerned shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions. In performing his or 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.

5. To the extent required, the Data Protection Officer shall be relieved of other activities. The Data Protection Officer and his or 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.

C.T.C.E. Piatra Neamț