Brussels, 15 December 2016
Case No: 68237
Document No: 802433
Decision No: 235/16/COL

EFTA SURVEILLANCE AUTHORITY

EFTA SURVEILLANCE AUTHORITY DECISION
of 15 December 2016
laying down Rules on Data Protection

THE EFTA SURVEILLANCE AUTHORITY,

HAVING REGARD to the agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice, in particular its Article 13,

Whereas:

In order to protect the fundamental right of natural persons to privacy, the natural persons should be provided with legally enforceable rights and the data processing obligations of the controllers within the EFTA Surveillance Authority ("The Authority") should be specified,

The persons to be protected are those whose personal data are processed by the Authority in any context whatsoever, including the staff of the Authority,

The data protection rules of the Authority should be aligned with those that apply to the EU institutions, laid down in 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,

Directive 95/46/EC requires the EEA EFTA 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 European Economic Area,

The Authority's handling of personal data should be subject to monitoring by the European Data Protection Supervisor in accordance with a working arrangement or agreement to be concluded with the Authority,

The Authority should take the necessary measures to inform the public of the new Rules on Data Protection and to train its staff in the processing of personal data and to assist natural persons to exercise their rights,

HAS ADOPTED THIS DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Decision

The EFTA Surveillance Authority shall protect the rights and freedoms of natural persons in accordance with this decision, and in particular their right to privacy with respect to the processing of personal data. The EFTA Surveillance Authority shall neither restrict nor prohibit the free flow of personal data to recipients, subject to EEA law on data protection and/or the national law of the Contracting Parties implementing any Union Act made part of the EEA Agreement relating to data protection.

Article 2

Definitions

For the purposes of this Decision:

(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 Authority or any organisational unit of the Authority:

(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 and monitoring by the European Data Protection Supervisor

1. This Decision shall apply to all processing of personal data by the Authority insofar as such processing is carried out in the exercise of activities, all or part of which fall within the scope of EEA law, including processing of personal data of staff.

2. This Decision 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.

3. The European Data Protection Supervisor shall monitor the application of the provisions of this Decision in accordance with an agreement or working arrangement to be concluded with the Authority.

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 be considered compatible 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 Authority may 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 EEA Agreement or legal acts incorporated into that Agreement; the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice (SCA); or in the legitimate exercise of official authority vested in the Authority 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 other internal rules of the Authority.

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 to EFTA Institutions that abide by similar data protection rules or EU institutions or bodies

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

1. Personal data may be transferred to the EFTA Court, the EFTA Secretariat and other EFTA institutions, or EU 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.

Article 8

Transfer of personal data to recipients, other than the EFTA Institutions that abide by similar data protection rules and EU 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 national law adopted pursuant to 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 the EFTA Institutions that abide by similar data protection rules and EU institutions and bodies, which are not subject to Directive 95/46/EC

1. Personal data shall only be transferred to recipients, other than EFTA or EU 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 Authority shall inform the European Data Protection Supervisor of cases where it considers the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2.

4. By way of derogation from paragraphs 1 and 2, the Authority 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 EEA 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 EEA law for consultation are fulfilled in the particular case.

5. The European Data Protection Supervisor may in any event 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.

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, 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 rules adopted on the basis of Article 13 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice, such as the Authority's Staff Rules and Regulations 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 defense of legal claims.

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 decided by the Authority after consultation with 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 EEA law subject to appropriate specific safeguards.

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,

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 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 EEA law.

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 the processing of that data 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 EEA law 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 Authority may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 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 Contracting Party to the EEA Agreement, 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 defense of the Contracting Parties to the EEA Agreement;

(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 Article 20(1) is imposed, the data subject shall be informed, in accordance with EEA 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, pursuant to a working agreement with the Authority, 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 Article 20(3) may be deferred for as long as such information would deprive the restriction imposed by Article 20(1) of its effect.

SECTION 7

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 21

Confidentiality of processing

A person employed by the Authority, with access to personal data, shall not process them except on instructions from the controller, unless required to do so by national or EEA 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 Contracting Parties to the EEA Agreement.

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. The Authority 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 Decision;

(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 Decision;

(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 Decision.

4. The Data Protection Officer shall be appointed for a term of up to three years. He or she shall be eligible for reappointment. He or she may be dismissed from the post of Data Protection Officer 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 Authority.

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

7. The Authority shall adopt rules concerning the mandate of the Data Protection Officer. These 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) an indication of the organisational part(s) of the Authority 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

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.

Article 28

Consultation

The Authority shall inform the European Data Protection Supervisor when drawing up administrative measures relating to the processing of personal data.

Article 29

Obligation to provide information

The Authority shall inform the European Data Protection Supervisor of the measures taken further to his or her decisions in accordance with any agreement or working arrangement concluded with the Authority.

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 information referred to in any agreement or working arrangement concluded with the Authority.

Article 31

Obligation to react to allegations

In response to decisions of the European Data Protection Supervisor concerning the Authority, the Authority 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. Any natural person, including staff of the Authority, may lodge a complaint with the European Data Protection Supervisor if he or she considers that his or her rights under this decision have been infringed as a result of the processing of his or her personal data by the Authority. If a complaint concerning the Authority's processing of personal data results in an opinion of the European Data Protection Supervisor, the Authority shall take the utmost account of the opinion in its decision. In the event that the Authority decides not to follow the opinion of the European Data Protection Supervisor, the Authority shall state the reasons on which its Decision is based and inform the parties and the European Data Protection Supervisor thereof.

2. The EFTA Court shall have jurisdiction to hear all disputes, which relate to the provisions of this Decision, in accordance with Article 36 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice.

3. Any person who has suffered damage because of an unlawful processing operation or any action incompatible with this Decision shall have the right to compensation in accordance with Article 46 of the Agreement between the EFTA States on the establishment of a Surveillance Authority and a Court of Justice.

Article 33

Complaints by Authority staff

Any person employed by the Authority may lodge a complaint with the European Data Protection Supervisor regarding an alleged breach of the provisions of this Decision 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 Decision, 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 the Authority.

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

Article 35

Security

1. The Authority 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 Authority shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.

Article 36

Confidentiality of communications

The Authority shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of EEA 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 may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. Those 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 necessary for the specific purposes of the directory.

2. The Authority 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 Authority shall inform the users thereof and of the possibilities set out in Article 39 (1), (2) and (3).

Article 40

Derogations

The Authority 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 VI

FINAL PROVISIONS

Article 41

Sanctions

Any failure to comply with the obligations pursuant to this Decision whether intentionally or through gross negligence on his or her part, shall make an official or other staff of the Authority liable to disciplinary action, in accordance with the rules and procedures laid down in the Authority's Staff Rules and Regulations or in the conditions of employment applicable to other staff.

Article 42

Transitional period

The Authority shall ensure that processing operations already under way on the date this Decision enters into force are brought into conformity with this Decision within one year of that date.

Article 43

Entry into force

This Decision shall enter into force on 1 January 2017.

Done at Brussels, 15 December 2016

For the EFTA Surveillance Authority

Sven Erik Svedman
President

Helga Jónsdóttir
College Member

This document has been electronically signed by Sven Erik Svedman, Helga Jonsdottir on 15/12/2016