ESA | EFTA Surveillance Authority

EFTA SURVEILLANCE AUTHORITY
RULES ON DATA PROTECTION

Adopted on 18 December 2019 by College Decision 100/19/COL

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter and objectives

These Rules regulate the protection of natural persons with regard to the processing of personal data by the Authority and free movement of personal data from the Authority to other recipients.

Article 2

Scope and monitoring by the European Data Protection Supervisor

1. These Rules apply to the 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. These Rules apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated 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 these Rules to all processing operations carried out by the Authority in accordance with a working arrangement with the Authority.

Article 3

Definitions

For the purposes of these Rules, the following definitions apply:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the Authority (ESA), which determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific EEA act, the controller or the specific criteria for its nomination can be provided for by EEA law;

(8) 'controllers other than Authority means controllers under Regulation (EU) 2018/1725, EFTA Court and EFTA Secretariat, controllers within the meaning of point (7) of Article 4 of Regulation (EU) 2016/679, controllers within the meaning of point (8) of Article 3 of Directive (EU) 2016/680;

(9) 'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty;

(10) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(11) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with EEA or EEA State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(12) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(13) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(14) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(15)'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(16)'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(17)'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status;

(18)'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[1];

(19)'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

(20)'national supervisory authority' means an independent public authority which is established by an EEA State pursuant to Article 51 of Regulation (EU) 2016/679;

(21)'user' means any natural person using a network or terminal equipment operated under the control of the Authority;

(22)'directory' means a publicly available directory of users or an internal directory of users available within the Authority, whether in printed or electronic form;

(23)'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(24)'terminal equipment' means terminal equipment as defined in point (1) of Article 1 of Commission Directive 2008/63/EC.[2]

(25)'third country' means a country other than the States party to the EEA Agreement

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, incorporated into EEA law by the EEA Joint Committee Decision 75/2019 of 29 March 2019 in point 1 of Chapter XIX of Annex II to the EEA Agreement with adaptations.

[2] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment; incorporated into EEA law by the EEA Joint Committee Decision 130/2010 of 10 December 2010 in point 4zzp of Chapter XVIII of Annex II to the EEA Agreement.

CHAPTER II
GENERAL PRINCIPLES

Article 4

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 14, not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 14 subject to implementation of the appropriate technical and organisational measures required by these Rules in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The Authority shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 5

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Authority;

(b) processing is necessary for compliance with a legal obligation to which the Authority is subject;

(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;

(d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

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

2. The basis for the processing referred to in points (a) and (b) of paragraph 1 must be laid down in 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 any acts adopted by the Authority on the legal basis set out therein.

Article 6

Processing for another compatible purpose

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on EEA law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 26(1), the Authority shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the Authority;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 11, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 12;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the Authority shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of these Rules shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on

consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to a child's consent in relation to information society services

1. Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2. The Authority shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general national contract law such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Transmission of personal data to EFTA institutions that abide by similar data protection rules or Union institutions or bodies

In accordance with the principle of accountability, and without prejudice to Articles 4 to 6 and 11, where the Authority transmits personal data to the EFTA Court, the EFTA Secretariat or another EFTA institution or body, provided they abide by similar data protection rules, or to a Union institution or body subject to Regulation (EU) 2018/1725, it shall verify whether such personal data are required for the legitimate performance of tasks within the competence of the recipient. In particular, following a recipient's request for transmission of personal data, the Authority shall verify the existence of a relevant ground for lawfully processing personal data and the competence of the recipient. The Authority shall also make a provisional evaluation of the necessity of the transmission of the data. If doubts arise as to this necessity, the Authority shall seek further information from the recipient. The recipient should ensure that the necessity of the transmission of the data can be subsequently verified.

Article 10

Transmissions of personal data to recipients established in the EEA other than those referred to in Article 9

1. Without prejudice to Articles 4 to 6 and 11, personal data shall only be transmitted to recipients established in the EEA other than those referred to in Article 9, if:

(a) the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient; or

(b) the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the Authority, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests.

2. Where the Authority initiates the transmission under this Article, it shall demonstrate that the transmission of personal data is necessary for and proportionate to the purposes of the transmission by applying the criteria laid down in points (a) or (b) of paragraph 1.

3. The Authority shall reconcile the right to the protection of personal data with the right of access to documents in accordance with EEA law.

Article 11

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where EEA law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Authority or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by EEA law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) the 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 consent;

(d) the 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 the Authority and with a political, philosophical, religious or trade union aim, such as the staff committee and on condition that the processing relates solely to the members or to former 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 outside that body without the consent of the data subjects;

(e) the processing relates to personal data which are manifestly made public by the data subject;

(f) the processing is necessary for the establishment, exercise or defence of legal claims;

(g)the processing is necessary for reasons of substantial public interest, on the basis of EEA law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h)the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EEA law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EEA law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EEA law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by, or under the responsibility of, a professional subject to the obligation of professional secrecy under EEA or the law of an EEA State or rules established by national competent bodies, or by another person also subject to an obligation of secrecy under EEA or EEA State law or rules established by national competent bodies.

Article 12

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 5(1) shall be carried out only under control of official authority or when the processing is authorised by EEA law providing for appropriate safeguards for the rights and freedoms of data subjects.

Article 13

Processing which does not require identification

1. If the purposes for which the Authority processes personal data do not or do no longer require the identification of a data subject by the Authority, the Authority shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with these Rules.

2. Where, in cases referred to in paragraph 1 of this Article, the Authority is able to demonstrate that it is not in a position to identify the data subject, it shall inform the data subject accordingly, if possible. In such cases, Articles 18 to 23 shall not apply

except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 14

Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with these Rules, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
Transparency and modalities

Article 15

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The Authority shall take appropriate measures to provide any information referred to in Articles 16 and 17 and any communication under Articles 18 to 25 and 35 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The Authority shall facilitate the exercise of data subject rights under Articles 18 to 25. In the cases referred to in Article 13(2), the Authority shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 18 to 25, unless the Authority demonstrates that it is not in a position to identify the data subject.

3. The Authority shall provide information on action taken on a request under Articles 18 to 25 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Authority shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the Authority does not take action on the request of the data subject, the Authority shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.

5. Information provided under Articles 16 and 17 and any communication and any actions taken under Articles 18 to 25 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Authority may refuse to act on the request. The Authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 13, where the Authority has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 18 to 24, the Authority may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 16 and 17 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

8. Where the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, the Authority may, where appropriate, provide the information pursuant to Articles 16 and 17 of these Rules in combination with such standardised icons.

SECTION 2

Information and access to personal data

Article 16

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the Authority shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a)the identity and the contact details of the controller;

(b)the contact details of the data protection officer;

(c)the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d)the recipients or categories of recipients of the personal data, if any;

(e)where applicable, the fact that the Authority intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in

Article 50 reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the Authority shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a)the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b)the existence of the right to request from the Authority access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

(c)where the processing is based on point (d) of Article 5(1) or point (a) of Article 11(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d)the right to lodge a complaint with the European Data Protection Supervisor;

(e)whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 25(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the Authority intends to further process the personal data for a purpose other than that for which the personal data were collected, the Authority shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 17

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the Authority shall provide the data subject with the following information:

(a)the identity and the contact details of the controller;

(b)the contact details of the data protection officer;

(c)the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d)the categories of personal data concerned;

(e)the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the Authority intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an

adequacy decision by the Commission, or in the case of transfers referred to in Article 48, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the Authority shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the Authority access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

(c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 11(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with the European Data Protection Supervisor;

(e) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(f) the existence of automated decision-making, including profiling, referred to in Article 25(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The Authority shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the Authority intends to further process the personal data for a purpose other than that for which the personal data were obtained, the Authority shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;

(c) obtaining or disclosure is expressly laid down by EEA law, which provides appropriate measures to protect the data subject's legitimate interests; or

(d)where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EEA law, including a statutory obligation of secrecy.

6. In the cases referred to in point (b) of paragraph 5 the Authority shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Article 18

Right of access by the data subject

1. The data subject shall have the right to obtain from the Authority confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a)the purposes of the processing;

(b)the categories of personal data concerned;

(c)the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d)where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e)the existence of the right to request from the Authority rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with the European Data Protection Supervisor;

(g)where the personal data are not collected from the data subject, any available information as to their source;

(h)the existence of automated decision-making, including profiling, referred to in Article 25(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 48 relating to the transfer.

3. The Authority shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

SECTION 3
Rectification and erasure

Article 19

Right to rectification

The data subject shall have the right to obtain from the Authority without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 20

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the Authority the erasure of personal data concerning him or her without undue delay and the Authority shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a)the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b)the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 11(2), and where there is no other legal ground for the processing;

(c)the data subject objects to the processing pursuant to Article 24(1) and there are no overriding legitimate grounds for the processing;

(d)the personal data have been unlawfully processed;

(e)the personal data have to be erased for compliance with a legal obligation to which the Authority is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the Authority has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the Authority, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers other than the Authority, which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a)for exercising the right of freedom of expression and information;

(b)for compliance with a legal obligation to which the Authority is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Authority;

(c)for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 11(2) as well as Article 11(3);

(d)for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e)for the establishment, exercise or defence of legal claims.

Article 21

Right to restriction of processing

1. The data subject shall have the right to obtain from the Authority restriction of processing where one of the following applies:

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

(b)the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c)the Authority no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d)the data subject has objected to processing pursuant to Article 24(1) pending the verification whether the legitimate grounds of the Authority override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EEA State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the Authority before the restriction of processing is lifted.

4. In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.

Article 22

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Authority shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 19, Article 20(1) and Article 21 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Authority shall inform the data subject about those recipients if the data subject requests it.

Article 23

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Authority, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Authority to which the personal data have been provided, where:

(a)the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 11(2) or on a contract pursuant to point (c) of Article 5(1); and

(b)the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from the Authority to another controller, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 20. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Authority.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

SECTION 4

Right to object and automated individual decision-making

Article 24

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (a) of Article 5(1), including profiling based on that provision. The Authority shall no longer process the personal data unless the Authority demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

3. Without prejudice to Articles 36 and 37, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using technical specifications.

4. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 25

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and the Authority;

(b) is authorised by EEA law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the Authority shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Authority, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 of this Article shall not be based on special categories of personal data referred to in Article 11(1), unless point (a) or (g) of Article 11(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

SECTION 5

Restrictions

Article 26

Restrictions

1. Legal acts adopted on the basis of the Treaties and incorporated into EEA Agreement or, in matters relating to the operation of the Authority, internal rules laid down by the latter may restrict the application of Articles 15 to 23, 35, and 36, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 15 to 23, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) the national security, public security or defence of the EEA States;

(b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(c) other important objectives of general public interest of the EEA State, in particular the objectives of the EEA Agreement and Surveillance and Court Agreement or an important economic or financial interest of the EEA State, including monetary, budgetary and taxation matters, public health and social security;

(d) the internal security of the Authority, including its electronic communications networks;

(e)the protection of judicial independence and judicial proceedings;

(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(g)a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c);

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

(i) the enforcement of civil law claims.

2. In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to:

(a)the purposes of the processing or categories of processing;

(b)the categories of personal data;

(c)the scope of the restrictions introduced;

(d)the safeguards to prevent abuse or unlawful access or transfer;

(e)the specification of the Authority or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; and

(g)the risks to the rights and freedoms of data subjects.

3. Where personal data are processed for scientific or historical research purposes or statistical purposes, EEA law, which may include internal rules adopted by the Authority in matters relating to its operation, may provide for derogations from the rights referred to in Articles 18, 19, 21 and 24 subject to the conditions and safeguards referred to in Article 14 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where personal data are processed for archiving purposes in the public interest, EEA law, which may include internal rules adopted by the Authority in matters relating to its operation, may provide for derogations from the rights referred to in Articles 18, 19, 21, 22, 23 and 24 subject to the conditions and safeguards referred to in Article 14 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

5. Internal rules referred to in paragraphs 1, 3 and 4 shall be clear and precise acts of general application, intended to produce legal effects vis-à-vis data subjects, adopted at the highest level of management of the Authority, subject to publication and challengeable by the persons concerned.

6. If a restriction is imposed pursuant to paragraph 1, 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 lodge a complaint with the European Data Protection Supervisor.

7. If a restriction imposed pursuant to 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.

8. Provision of the information referred to in paragraphs 6 and 7 of this Article and in Article 45(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 of this Article.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
General obligations

Article 27

Responsibility of the Authority as a controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Authority shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with these Rules. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the Authority.

3. Adherence to approved certification mechanisms as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the obligations of the Authority.

Article 28

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the Authority shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of these Rules and protect the rights of data subjects.

2. The Authority shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal

data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 of Regulation (EU) 2016/679 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 29

Joint controllers

1. Where the Authority together with one or more controllers other than the Authority jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 16 and 17, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by EEA or EEA State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under these Rules in respect of and against each of the controllers.

Article 30

Processor

1. Where processing is to be carried out on behalf of the Authority, the Authority shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of these Rules and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the Authority. In the case of general written authorisation, the processor shall inform the Authority of any intended changes concerning the addition or replacement of other processors, thereby giving the Authority the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under EEA or EEA State law, that is binding on the processor with regard to the Authority and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the Authority. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the Authority, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EEA or EEA State law to which the processor is subject; in such a case, the processor shall inform the

Authority of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 33;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the Authority by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Authority's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the Authority in ensuring compliance with the obligations pursuant to Articles 33 to 41 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the Authority, deletes or returns all the personal data to the Authority after the end of the provision of services relating to processing, and deletes existing copies unless EEA or EEA State law requires storage of the personal data;

(h) makes available to the Authority all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Authority or another auditor mandated by the Authority.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the Authority if, in its opinion, an instruction infringes these Rules or other EEA or national data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the Authority, the same data protection obligations as set out in the contract or other legal act between the Authority and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under EEA or EEA State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these Rules. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the Authority for the performance of that other processor's obligations.

5. When a processor is not the Authority, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to any individual contract between the Authority and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than the Authority pursuant to Article 42 of Regulation (EU) 2016/679.

7. The Authority may choose to use the Commission's standard contractual clauses which were adopted for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 96(2) of Regulation 2018/1725.

8. The Authority may choose to use the European Data Protection Supervisor standard contractual clauses for the matters referred to in paragraphs 3 and 4.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 53, if a processor infringes these Rules by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 31

Processing under the authority of the Authority or processor

The processor and any person acting under the authority of the Authority or of the processor, who has access to personal data, shall not process those data except on instructions from the Authority, unless required to do so by EEA or EEA State law.

Article 32

Records of processing activities

1. The Authority shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in EEA States, third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 33.

2. When acting as processor, the Authority shall maintain a record of all categories of processing activities carried out on behalf of a Authority, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

(d)where possible, a general description of the technical and organisational security measures referred to in Article 33.

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The Authority shall make the record available to the European Data Protection Supervisor on request.

5. The Authority shall keep its records of processing activities in a central register. It shall make the register publicly accessible.

SECTION 2

Security of personal data

Article 33

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Authority and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

(a)the pseudonymisation and encryption of personal data;

(b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. The Authority and processor shall take steps to ensure that any natural person acting under the authority of the Authority or the processor who has access to personal data does not process them except on instructions from the Authority, unless he or she is required to do so by EEA law.

4. Adherence to an approved certification mechanism as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Article 34

Notification of a personal data breach to the European Data Protection Supervisor

1. In the case of a personal data breach, the Authority shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the Authority without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the Authority to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The Authority shall inform the data protection officer about the personal data breach.

6. The Authority shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article.

Article 35

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Authority shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 34(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the Authority has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the

personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the Authority has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the Authority has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

SECTION 3

Confidentiality of electronic communications

Article 36

Confidentiality of electronic communications

The Authority shall ensure the confidentiality of electronic communications, in particular by securing its electronic communications networks and terminal equipment.

Article 37

Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment

The Authority shall protect the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC[3].

Article 38

Directories of users

1. Personal data contained in 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 Authority shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes regardless of whether they are accessible to the public or not.

[3] Incorporated into EEA law by the decision of the EEA Joint Committee 80/2003 of 20 June 2003 in point 5ha of the Annex XI to the EEA Agreement.

SECTION 4

Data protection impact assessment and prior consultation

Article 39

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Authority shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The Authority shall seek the advice of the data protection officer when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 11, or of personal data relating to criminal convictions and offences referred to in Article 12; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

(d) processing operations included on the list established by the European Data Protection Supervisor in accordance with Article 39(4) of Regulation (EU) 2018/1725

4. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with these Rules taking into account the rights and legitimate interests of data subjects and other persons concerned.

5. Compliance with approved codes of conduct referred to in Article 40 of Regulation (EU) 2016/679 by the relevant processors other than the Authority shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.

6. Where appropriate, the Authority shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of public interests or the security of processing operations.

7. Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties and incorporated into EEA legal order, which regulates the specific processing operation or set of operations in question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 of this Article shall not apply unless that legal act provides otherwise.

8. Where necessary, the Authority shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 40

Prior consultation

1. The Authority shall consult the European Data Protection Supervisor prior to processing where a data protection impact assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the Authority is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation. The Authority shall seek the advice of the data protection officer on the need for prior consultation.

2. When consulting the European Data Protection Supervisor pursuant to paragraph 1, the Authority shall provide the European Data Protection Supervisor with:

(a)where applicable, the respective responsibilities of the Authority, joint controllers and processors involved in the processing;

(b)the purposes and means of the intended processing;

(c)the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d)the contact details of the data protection officer;

(e)the data protection impact assessment provided for in Article 39; and

(f) any other information requested by the European Data Protection Supervisor.

3. The Authority shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing of personal data for the performance of a task carried out by the Authority in the public interest, including the processing of such data in relation to social protection and public health in cases determined by the Commission in an implementing act upon its incorporation into the EEA law.

SECTION 5
Information and cooperation

Article 41

Information and consultation with the European Data Protection Supervisor

1. The Authority shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data by the Authority, whether alone or jointly with others.

2. The Authority shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 26.

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

Article 42

Obligation to cooperate with the European Data Protection Supervisor

1. At his or her request, Authority 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.

2. 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.

SECTION 6
Data protection officer

Article 43

Designation of the data protection officer

1. The Authority shall designate a data protection officer.

2. The Authority may designate a single data protection officer or several of them, taking into account its organisational structure and size.

3. The data protection officer shall be a staff member of the Authority and without prejudice to these Rules subject to the rules and regulations applicable to officials of the Authority.

4. The data protection officer shall be designated on the basis of professional qualities and in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 45.

5. The Authority shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.

Article 44

Position of the data protection officer

1. The Authority shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The Authority shall support the data protection officer in performing the tasks referred to in Article 45 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The Authority shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the Authority or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the Authority.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under these Rules.

5. The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with EEA law.

6. The data protection officer may fulfil other tasks and duties. The Authority or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

7. The data protection officer may be consulted by the Authority and the processor, by the staff committee concerned and by any individual on any matter concerning the interpretation or application of these Rules, without them going through the official channels. 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 these Rules has taken place.

8. The data protection officer shall be designated for a term of three years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Authority, acting upon a proposal from the Director of Legal and Executive Affairs in agreement with the Director of Administration 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.

9. After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Authority.

Article 45

Tasks of the data protection officer

1. The data protection officer shall have the following tasks:

(a)to inform and advise the Authority or the processor and the employees who carry out processing of their obligations pursuant to these Rules and to other EEA law data protection provisions;

(b)to ensure in an independent manner the internal application of these Rules; to monitor compliance with these Rules, with other applicable EEA law containing data protection provisions and with the policies of the Authority or processor in relation

to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;

(c) to ensure that data subjects are informed of their rights and obligations pursuant to these Rules;

(d) to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35;

(e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment;

(f) to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;

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

(h) to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

2. The data protection officer may make recommendations to the Authority and the processor for the practical improvement of data protection and advise them on matters concerning the application of data protection provisions. Furthermore, in accordance with the investigation procedure to be set out in the implementing rules, he or she may, on his or her own initiative or at the request of the Authority or the processor, the staff committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice, and report back to the person who commissioned the investigation or to the Authority or the processor.

3. Further implementing rules concerning the data protection officer may be adopted by the Authority. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.

CHAPTER V

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 46

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of these Rules, the conditions laid down in this Chapter are complied with by the Authority and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this

Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by these Rules is not undermined.

Article 47

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection and where the personal data are transferred solely to allow tasks within the competence of the Authority to be carried out and upon incorporation of such decision into EEA law.

2. The Authority shall take the necessary measures to comply with decisions taken by the Commission where it establishes, pursuant to Article 45(3) or (5) of Regulation (EU) 2016/679, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures or no longer ensures an adequate level of protection.

Article 48

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 the Authority may transfer personal data to a third country or to an international organisation only if the Authority or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) standard data protection clauses adopted by the Commission;

(c) standard data protection clauses adopted by the European Data Protection Supervisor;

(d) where the processor is not the Authority, EFTA Court, the EFTA Secretariat and other EFTA institutions or bodies, or Union institutions or bodies, binding corporate rules, codes of conduct or certification mechanisms pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679.

3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the Authority or processor and the Authority, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The Authority shall inform the European Data Protection Supervisor of the categories of cases in which this Article has been applied.

Article 49

Transfers or disclosures not authorised by EEA law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring the Authority to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EEA State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 50

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or of appropriate safeguards pursuant to Article 48 of these Rules a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a)the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

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

(c)the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Authority and another natural or legal person;

(d)the transfer is necessary for important reasons of public interest;

(e)the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g)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, but only to the extent that the conditions laid down in EEA law for consultation are fulfilled in the particular case.

2. Points (a), (b) and (c) of paragraph 1 shall not apply to activities carried out by the Authority in the exercise of its public powers.

3. The public interest referred to in point (d) of paragraph 1 shall be one recognised in EEA law.

4. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless

authorised by EEA law. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

5. The Authority shall inform the European Data Protection Supervisor of the categories of cases in which this Article has been applied.

CHAPTER VI
REMEDIES AND LIABILITY

Article 51

Right to lodge a complaint with the European Data Protection Supervisor

1. Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that if the data subject considers that his or her rights under these Rules have been infringed as a result of the processing of his or her personal data by the Authority.

2. 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 personal data subjects and the European Data Protection Supervisor thereof.

3. Any person employed by the Authority may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of these Rules, including without acting through official channels. No one shall suffer prejudice by reason of having submitted a complaint with the European Data Protection Supervisor alleging such an infringement.

Article 52

Right to an effective judicial remedy

The EFTA Court shall have jurisdiction to hear all disputes relating to the provisions of these Rules, in accordance with Article 36 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice.

Article 53

Compensation

Any person who has suffered material or non-material damage as a result of an infringement of these Rules shall have the right to receive compensation from the Authority for the damage suffered, 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 54

Sanctions

Where an official or other servant of the Authority fails to comply with the obligations laid down in these Rules, whether intentionally or through gross negligence on his or her part, the official or other servant concerned shall be liable to disciplinary or other action, in accordance with the rules and procedures laid down in the Staff Regulations or in the conditions of employment applicable to other staff.

CHAPTER VII
FINAL PROVISIONS

Article 55

Status of Decision 235/16/COL of 15 December 2016 laying down Rules on Data Protection and Decision 236/16/COL of 15 December 2016 laying down the mandate for the Data Protection Officer

1. EFTA Surveillance Authority Decision No 235/16/COL of 15 December 2016 laying down Rules on Data Protection ('Decision No 235/16/COL'), with the exception of Article 7 thereof, is repealed and replaced by the Decision adopting the present Rules. All references in other Authority documentation to Decision No 235/16/COL shall insofar as possible be construed as references to the present Rules.

2. As regards transmission of personal data to the EFTA Secretariat and the EFTA Court, Article 7 of Decision No 235/16/COL remains in force and shall take precedence over the present Rules until such time as it is repealed by a decision of the Authority.

3. EFTA Surveillance Authority Decision No 236/16/COL of 15 December 2016 laying down the mandate for the Data Protection Officer ('Decision No 236/16/COL') remains in force until such time as it is repealed by a decision of the Authority. However, in instances of conflict between Decision No 236/16/COL and the present Rules, the present Rules shall take precedence.

Article 56

Transitional measures

1. The Authority shall ensure that processing operations already under way on the date the present Rules enter into force are brought into conformity with these rules within one year of that date.
2. The Authority shall adopt all necessary implementing measures within one year of the entry into force of the present Rules.

Article 57

Entry into force and application

These Rules shall enter into force on 1 January 2020 and shall thereafter be binding upon the Authority.