REGULATION (EU) No XXX/2016
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
(Text with EEA relevance)

This version includes a Table of Contents and some space for your personal notes.

It was prepared **by Cabinet Cilex, a French consultancy**
dedicated to Data Protection Officers
and Privacy Compliance in Europe.

Proud member of www.privacy-europe.com

This document is a small part of the
Documentation provided in our Workshops
about the new Regulation.

You can reach us on http://www.cabinet-cilex.com and contact@cabinet-cilex.com .

We provide consulting, training, software to manage the DPO's documentation,
and external Data Protection Officers.

This document is version 1.0. -
we hope that you'll find it convenient
to work on this new Regulation
and to prepare your future compliance.
Please contact us if you have ideas to enhance this version !

Your Notes

Your Notes

Content

Your Notes

Your Notes

Your Notes

Your Notes

Article 1 - Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

2a. (…)

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article 2 - Material scope

1. This Regulation applies 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.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) (…)

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;

(d) by a natural person in the course of a purely personal or household activity;

(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2a. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 90a.

3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3 - Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4 - Definitions For the purposes of this Regulation:

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

(2) (…)

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

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

(3aa) 'profiling' means any form of automated processing of personal data consisting of using those 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;

(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person;

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

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

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

Your Notes

(7) 'recipient' means a natural or legal person, public authority, agency or any other 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 Union or Member State law shall not be regarded as recipients; the processing of these data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

(7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(8) 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) '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;

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.

(12a) (…)

(13) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in this case the establishment having taken such decisions shall be considered as the main establishment;.

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Your Notes

(14) 'representative' means any natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 25, represents the controller or processor, with regard to their respective obligations under this Regulation;

(15) 'enterprise' means any natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or group of enterprises engaged in a joint economic activity;

(18) (…)

(19) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 46;

(19a) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing, because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in this Member State are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged to that supervisory authority.

(19b) 'cross-border processing of personal data' means either:

(a) processing which takes place in the context of the activities of establishments in more than one Member State of a controller or a processor in the Union and the controller or processor is established in more than one Member State; or

(b) processing which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(19c) 'relevant and reasoned objection' means: an objection as to whether there is an infringement of this Regulation or not, or, as the case may be, whether the envisaged action in relation to the controller or processor is in conformity with the Regulation. The objection shall clearly demonstrate the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and where applicable, the free flow of personal data within the Union;

(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services;

Your Notes

(21) '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.

Your Notes

Your Notes

Article 5 - Principles relating to personal data processing

1. Personal data must 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 way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1), not be considered 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 data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

(eb) processed in a way 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");

(ee) (…)

(f) (…)

2. The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

Article 6 - Lawfulness of processing

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

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) 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;

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

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

(e) 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 controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. (…)

2a. (new) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 must be laid down by:

(a) Union law, or

(b) Member State law to which the controller is subject. The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX. The Union law or the Member State law must meet an objective of public interest and be proportionate to the legitimate aim pursued.

3a. Where the processing for another purpose than the one for which the data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in points (aa) to (g) of Article 21(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the 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 controller;

Your Notes

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 or whether data related to criminal convictions and offences are processed, pursuant to Article 9a;

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

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

4. (…)

5. (…)

Your Notes

Article 7 - Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that consent was given by the data subject to the processing of their personal data.

1a. (…)

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 must 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 the declaration which constitutes an infringement of this Regulation that the data subject has given consent to 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 consent as to give it.

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

Article 8 - Conditions applicable to child's consent in relation to information society services

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 16 years, or if provided for by Member State law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child.

1a. The controller 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.

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

3. (…)

4. (…).

Article 9 - Processing of special categories of personal data

Your Notes

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and 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 Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union law or Member State law or a collective agreement pursuant to Member State law providing for adequate safeguards for the fundamental rights and the interests of the data subject; or

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

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the 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; or

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

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State 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; or

(h) 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 Union law or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 4; or

(hb) 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 health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(i) processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) based on Union or Member State 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.

(j) (…)

3. (…)

4. 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 Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

5. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.

Article 9a - Processing of data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions may be kept only under the control of official authority.

Article 10 - Processing not requiring identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller 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 this Regulation.

2. Where, in such cases the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.

Your Notes

Your Notes

SECTION 1 - TRANSPARENCY AND MODALITIES

Article 11 - Transparent information and communication

1. (…)

2. (…)

Article 12 - Transparent information, communication and modalities for exercising the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Article 14 and 14a and any communication under Articles 15 to 20, and 32 relating to the processing of personal data 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, where appropriately in electronic form. When requested by the data subject, the information may be given orally provided that the identity of the data subject is proven by other means.

1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 20. In cases referred to in Article 10(2) the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 20, unless the controller demonstrates that it is not in a position to identify the data subject.

2. The controller shall provide information on action taken on a request under Articles 15 to 20 to the data subject without undue delay and, at the latest within one month of receipt of the request. This period may be extended for a maximum of two further months when necessary, taking into account the complexity of the request and the number of the requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay. Where the data subject makes the request in electronic form, the information shall be provided in electronic form where possible, unless otherwise requested by the data subject.

3. If the controller does not take action on the request of the data subject, the controller 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 to a supervisory authority and seeking a judicial remedy.

4. Information provided under Articles 14 and 14a and any communication and any actions taken under Articles 15 to 20 and 32 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 controller may charge a reasonable fee taking into account the administrative costs for providing the information or the communication or taking the action requested, or the controller may refuse to act on the request. In these cases, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

4b. The information to be provided to data subjects pursuant to Article 14 and 14a may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible way a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

4c. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

5. (…)

6. (…).

Article 13 - Rights in relation to recipients (…)

SECTION 2 - INFORMATION AND ACCESS TO DATA

Article 14 - Information to be provided where the data are collected from the data subject

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

(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall also include the contact details of the data protection officer, if any;

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

(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(d) where applicable, the recipients or categories of recipients of the personal data;

(e) where applicable, that the controller 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 case of transfers referred to in Article 42 or 43, or point (h) of Article 44(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;

1a. In addition to the information referred to in paragraph 1, the controller 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 this is not possible, the criteria used to determine this period;

(b) …

Your Notes

(c) …

(d) …

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject or to object to the processing of such personal data as well as the right to data portability;

(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(f) the right to lodge a complaint to a supervisory authority;

(g) 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 data and of the possible consequences of failure to provide such data;

(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) 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.

1b. Where the controller intends to further process the data for a purpose other than the one for which the data were collected the controller 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 1a.

2. (…)

3. (…)

4. (…)

5. Paragraphs 1, 1a and 1b shall not apply where and insofar as the data subject already has the information.

6. (…)

7. (…)

8. (…).

Article 14a - Information to be provided where the data have not been obtained from the data subject

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

(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall also include the contact details of the data protection officer, if any;

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

Your Notes

(ba) the categories of personal data concerned;

(c) (…)

(d) where applicable, the recipients or categories of recipients of the personal data;

(da) where applicable, that the controller 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 case of transfers referred to in Article 42 or 43, or point (h) of Article 44(1), 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 controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

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

(ba) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) (…)

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data as well as the right to data portability;

(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(f) the right to lodge a complaint to a supervisory authority;

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

(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) 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 controller shall provide the information referred to in paragraphs 1 and 2:

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

(b) if the 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 data are first disclosed.

Your Notes

3a. Where the controller intends to further process the data for a purpose other than the one for which the data were obtained, the controller 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 to 3a shall not apply where and insofar as:

(a) the data subject already has the information; or

(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, or scientific and historical research purposes or statistical purposes subject to the conditions and safeguards referred to in Article 83(1) or 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 the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes; in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; or

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

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

Article 15 - Right of access for the data subject

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

(a) the purposes of the processing;

(b) the categories of personal data concerned;

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

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

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

(f) the right to lodge a complaint to a supervisory authority;

(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 20(1) and (3) 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.

Your Notes

1a. 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 42 relating to the transfer.

1b. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request in electronic form, and unless otherwise requested by the data subject, the information shall be provided in an electronic form, which is commonly used.

2. (…)

2a. The right to obtain a copy referred to in paragraph 1b shall not adversely affect the rights and freedoms of others.

3. (…)

4. (…).

SECTION 3 - RECTIFICATION AND ERASURE

Article 16 - Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

Article 17 - Right to erasure ("right to be forgotten")

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

(a) the 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 (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);

(d) they have been unlawfully processed;

(e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

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

1a. (…)

2. (…)

Your Notes

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

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

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

(b) for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller 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 controller;

(c) for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (hb) as well as Article 9(4);

(d) for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) 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 the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes. (e) for the establishment, exercise or defence of legal claims.

4. (…)

5. (…)

6. (…)

7. (…)

8. (…)

9. (…)

Article 17a - Right to restriction of processing

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

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

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

(b) the controller 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; or

(c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Your Notes

2. Where processing of personal data has been restricted under paragraph 1, such data may, 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 Union or of a Member State.

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

Article 17b - Notification obligation regarding rectification, erasure or restriction

The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests this.

Article 18 - Right to data portability

1. (…)

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

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and

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

2a. (new) In exercising his or her right to data portability pursuant to paragraph 1, the data subject has the right to obtain that the data is transmitted directly from controller to controller where technically feasible.

2a. The exercise of this right shall be without prejudice to Article 17. The right referred to in paragraph 2 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 controller.

2aa. The right referred to in paragraph 2 shall not adversely affect the rights and freedoms of others.

3. (…)

SECTION 4 - RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION MAKING

Article 19 - 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 the processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on these provisions. The controller shall no longer process the personal data unless the

Your Notes

controller 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. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

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

2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

2aa. Where personal data are processed for scientific and historical research purposes or statistical purposes pursuant to Article 83(1), 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.

3. (…).

Article 20 - 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.

1a. Paragraph 1 shall not apply if the decision:

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

(b) is authorized by Union or Member State law to which the controller is subject and 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.

1b. In cases referred to in paragraph 1a (a) and (c) the data controller 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 controller, to express his or her point of view and to contest the decision.

2. (…)

3. Decisions referred to in paragraph 1a shall not be based on special categories of personal data referred to in Article 9(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4. (…)

Your Notes

5. (…)

Your Notes

SECTION 5 - Restrictions

Article 21 - Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 20 and Article 32, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, 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:

(aa) national security;

(ab) defence;

(a) public security;

(b) the prevention, investigation, detection or 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 interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

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

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

(e) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in cases referred to in (aa), (ab), (a), (b), (c) and (d);

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

(g) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, 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 controller 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;

(g) the risks for the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless this may be prejudicial to the purpose of the restriction.

Your Notes

Your Notes

SECTION 1 - GENERAL OBLIGATIONS

Article 22 - Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary.

2. (…)

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

2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.

3. (…)

4. (…)

Article 23 - Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller 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 way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller 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; this applies to the amount of 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 individuals.

2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

3. (…)

4. (…)

Article 24 - Joint controllers

1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, 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 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a point of contact for data subjects.

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

3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject.

Article 25 - Representatives of controllers not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. This obligation shall not apply to:

(a) (…);

(b) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences referred to in Article 9a, and is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing; or

(c) a public authority or body.

(d) (…)

3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.

3a. The representative shall be mandated by the controller or the processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.

4. The designation of a representative by the controller or the processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 26 - Processor

1. Where a processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the

Your Notes

processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting 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, the obligations and rights of the controller and stipulating in particular that the processor shall:

(a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;

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

(c) take all measures required pursuant to Article 30;

(d) respect the conditions referred to in paragraphs 1a and 2a for enlisting another processor;

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

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data;

(h) make available to the controller 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 controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.

2a. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement

Your Notes

appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate sufficient guarantees referred to in paragraphs 1 and 2a.

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c, including when they are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).

2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.

4. Without prejudice to Articles 77, 79 and 79b, if a processor in breach of this Regulation determines the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing.

5. (…).

Article 27 - Processing under the authority of the controller and processor

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

Article 28 - Records of processing activities

1. Each controller and, if any, the controller's representative, shall maintain a record of processing activities under its responsibility. This record shall contain the following information:

(a) the name and contact details of the controller and any joint controller, the controller's representative and the data protection officer, if any;

(b) (…)

(c) the purposes of the processing;

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

(e) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;

Your Notes

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

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

(h) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

2a. Each processor and, if any, the processor's representative shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, 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 controller's or the processor's representative, and the data protection officer, if any;

(b) (…)

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

(d) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

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

3. Upon request, the controller and the processor and, if any, the controller's or the processor's representative, shall make the record available to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2a shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk for the rights and freedoms of data subject, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences referred to in Article 9a.

5. (…)

6. (…).

Article 29 - Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller or the processor, shall co-operate, on request, with the supervisory authority in the performance of its tasks.

2. (…).

Your Notes

SECTION 2 - DATA SECURITY

Your Notes

Article 30 - Security of processing

1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller 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 systems and services processing personal data;

(c) the ability to restore the availability and access to 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.

1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. (…)

2a. Adherence to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.

2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3. (…)

4. (…).

Article 31 - Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller 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 supervisory authority competent in accordance with Article 51, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

1a. (…)

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

3. The notification referred to in paragraph 1 must 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 data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) (…)

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

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

(f) (…)

3a. 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.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article.

5. (…)

6. (…)

Article 32 - Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk the rights and freedoms of individuals the controller 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 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (d) and (e) of Article 31(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if:

(a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

(b) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or (c) it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Your Notes

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the breach to result 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.

5. (…)

6. (…).

SECTION 3 - DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 33 - 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 for the rights and freedoms of individuals, the controller 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.

1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:

(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 individual or similarly significantly affect the individual;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of data relating to criminal convictions and offences referred to in Article 9a;

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

(d) (…)

(e) (…)

2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board.

2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.

2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are

Your Notes

related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

3. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller;

(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;

(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 this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

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

5. Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law, or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been made as part of a general impact assessment in the context of the adoption of this legal basis, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. (…)

7. (…)

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

Article 34 - Prior consultation

1. (…)

2. The controller shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it shall within a maximum period of eight weeks following the request for consultation give advice to the data

Your Notes

controller, and where applicable the processor in writing, and may use any of its powers referred to in Article 53. This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller, and where applicable the processor shall be informed within one month of receipt of the request including of the reasons for the delay. These periods may be suspended until the supervisory authority has obtained any information it may have requested for the purposes of the consultation.

4. (…)

5. (…)

6. When consulting the supervisory authority pursuant to paragraph 2, the controller shall provide the supervisory authority with

(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(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) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 33; and

(f) any other information requested by the supervisory authority.

7. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the processing of personal data.

7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.

8. (…)

9. (…).

SECTION 4 - DATA PROTECTION OFFICER

Article 35 - Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or

Your Notes

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and data relating to criminal convictions and offences referred to in Article 9a.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. 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 37.

6. (…)

7. (…)

8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority.

10. (…)

11. (…).

Article 36 - Position of the data protection officer

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

2. The controller or processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations, and to maintain his or her expert knowledge.

2a. (new) Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.

3. The controller or processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of these tasks. He or she shall not be dismissed or penalised by the controller or the

Your Notes

processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

4a. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 37 - Tasks of the data protection officer

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

(a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;

(c) (…)

(d) (…)

(e) (…)

(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

(g) to cooperate with the supervisory authority;

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter.

2. (…)

2a. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

SECTION 5 - CODES OF CONDUCT AND CERTIFICATION

Article 38 - Codes of conduct

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.

Your Notes

1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(a) fair and transparent data processing;

(aa) the legitimate interests pursued by controllers in specific contexts;

(b) the collection of data;

(bb) the pseudonymisation of personal data;

(c) the information of the public and of data subjects;

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

(e) information and protection of children and the way to collect the consent of the holder of parental responsibility over the child;

(ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security of processing referred to in Article 30;

(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;

(f) transfer of personal data to third countries or international organisations;

(g) (…)

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct approved pursuant to paragraph 2 and having general validity pursuant to paragraph 4 may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including as regards data subjects' rights.

1b. Such a code of conduct pursuant to paragraph 1a shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended

Your Notes

code is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.

3. Where the opinion referred to in paragraph 2b confirms that the codes of conduct, or amended or extended codes, is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission.

4. The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 4.

5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means.

Article 38a - Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38, may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

2. A body referred to in paragraph 1 may be accredited for this purpose if:

(a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;

Your Notes

(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body referred to in paragraph 1 shall, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Article 39 - Certification

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including as regards data subjects' rights.

1b. The certification shall be voluntary and available via a process that is transparent.

2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2a. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 39a, or by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board. In the latter case, the criteria approved by the European Data Protection Board may result in a common certification, the European Data Protection Seal.

Your Notes

3 (new). The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn, where applicable, by the certification bodies referred to in Article 39a, or by the competent supervisory authority where the requirements for the certification are not or no longer met.

5. The European Data Protection Board shall collect all certification mechanisms and data protection seals and marks in a register and shall make them publicly available through any appropriate means.

Article 39a - Certification body and procedure

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed, after informing the supervisory authority in order to allow the exercise of its powers pursuant to Article 53(1b)(fa) where necessary, by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:

(a) the supervisory authority which is competent according to Article 51 or 51a; and/or

(b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European Parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.

2. The certification body referred to in paragraph 1 may be accredited for this purpose only if:

(a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(aa) it has undertaken to respect the criteria referred to in paragraph 2a of Article 39 and approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board;

(b) it has established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;

(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

Your Notes

3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board. In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.

5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 and the criteria referred to in paragraph 2a of Article 39 shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means.

6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1 of Article 39.

7a. (…)

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Your Notes

CHAPTER V - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40 - 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 may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller 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 individuals guaranteed by this Regulation shall not be undermined.

Article 41 - Transfers with an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of this legislation, data protection rules professional rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, jurisprudential precedents, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments

in the third country or international organisation. The implementing act shall specify its territorial and sectorial application and, where applicable, identify the supervisory authority or authorities mentioned in point(b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

3a. (…)

4. (…)

4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3, decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 without retro-active effect. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 87(3).

5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44.

7. The Commission shall publish in the Official Journal of the European Union and on its website a list of those third countries, territories and specified sectors within a third country and international organisations where it has decided that an adequate level of protection is or is no longer ensured.

8. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5.

Article 42 - Transfers by way of appropriate safeguards

1. In the absence of a decision pursuant to paragraph 3 of Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced 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 a supervisory authority, by:

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

(a) binding corporate rules in accordance with Article 43; or

Your Notes

(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 87(2); or

(d) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the 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.

3. (…)

4. (…)

5. (…)

5a. The supervisory authority shall apply the consistency mechanism referred to in Article 57 in the cases referred to in paragraph 2a.

5b. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2.

Article 43 - Transfers by way of binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 57, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings or groups of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

Your Notes

(a) the structure and contact details of the concerned group and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (i) of this paragraph;

Your Notes

(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(m) the appropriate data protection training to personnel having permanent or regular access to personal data.

2a. (…)

3. (…)

4. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 43a (new) - Transfers or disclosures not authorised by Union law

1. Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor 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 Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 44 - Derogations for specific situations

1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(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; or

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

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

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

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

(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 Union or Member State 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 Union or Member State law for consultation are fulfilled in the particular case; or

Your Notes

(h) Where a transfer could not be based on a provision in Articles 41 or 42, including binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall in addition to the information referred to in Article 14 and Article 14a, inform the data subject about the transfer and on the compelling legitimate interests pursued by the controller.

2. 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. When 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.

3. (…)

4. Points (a), (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in point (h) of paragraph 1 in the records referred to in Article 28.

7. (…).

Article 45 - International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

Your Notes

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

2. (…)

Your Notes

Your Notes

SECTION 1 - INDEPENDENT STATUS

Article 46 - Supervisory authority

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union.

1a. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission in accordance with Chapter VII.

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which shall represent those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 47 - Independence

1. Each supervisory authority shall act with complete independence in performing the tasks and exercising the powers entrusted to it in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. (…)

5. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.

6. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, annual budgets, which may be part of the overall state or national budget.

Your Notes

Article 48 - General conditions for the members of the supervisory authority

1. Member States shall provide that each member of a supervisory authority must be appointed by means of a transparent procedure either: - by the parliament; or - the government; or - the head of State of the Member State concerned; or - by an independent body entrusted by Member State law with the appointment.

2. The member or members shall have the qualifications, experience and skills, notably in the area of protection of personal data, required to perform their duties and exercise their powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the law of the Member State concerned.

4. A member may only be dismissed in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 49 - Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority which shall not be less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority shall be eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

(g) (…)

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, this duty of professional secrecy shall in particular apply to reporting by individuals of infringements of this Regulation.

Article 50 - Professional secrecy (...)

Your Notes

SECTION 2 - COMPETENCE, TASKS AND POWERS

Article 51 - Competence

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 51a does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 51a - Competence of the lead supervisory authority

1. Without prejudice to Article 51, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing of this controller or processor in accordance with the procedure provided in Article 54a.

2a. By derogation from paragraph 1, each supervisory authority shall be competent to deal with a complaint lodged with it or to deal with a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

2b. In the cases referred to in paragraph 2a, the supervisory authority shall inform the lead supervisory authority without delay on this matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will deal with the case in accordance with the procedure provided in Article 54a, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

2c. Where the lead supervisory authority decides to deal with the case, the procedure provided in Article 54a shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in paragraph 2 of Article 54a.

2d. In case the lead supervisory authority decides not to deal with it, the supervisory authority which informed the lead supervisory authority shall deal with the case according to Articles 55 and 56.

3. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing of that controller or processor.

Article 52 - Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;

(ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(ac) promote the awareness of controllers and processors of their obligations under this Regulation;

(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;

(b) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 76, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) cooperate with, including sharing information and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(d) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

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

(f) adopt standard contractual clauses referred to in Article 26(2c) and 42(2)(c);

(fa) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);

(g) give advice on the processing operations referred to in Article 34(3);

(ga) encourage the drawing up of codes of conduct pursuant to Article 38 and give an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 38 (2);

(gb) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 39(1), and approve the criteria of certification pursuant to Article 39 (2a);

(gc) where applicable, carry out a periodic review of certifications issued in accordance with Article 39(4);

(h) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 38 a and of a certification body pursuant to Article 39a;

(ha) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;

(hb) authorise contractual clauses and provisions referred to in Article 42(2a);

(i) approve binding corporate rules pursuant to Article 43;

Your Notes

(j) contribute to the activities of the European Data Protection Board;

(jb) to keep internal records of breaches of this Regulation and of measures taken, in particular warnings issued and sanctions imposed;

(k) fulfil any other tasks related to the protection of personal data.

2. (…)

3. (…)

4. Each supervisory authority shall facilitate the submission of complaints referred to in point (b) of paragraph 1, by measures such as a complaint submission form, which can be completed also electronically, without excluding other means of communication.

5. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer, if any.

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 53 - Powers

1. Each supervisory authority shall have the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(aa) to carry out investigations in the form of data protection audits;

(ab) to carry out a review on certifications issued pursuant to Article 39(4);

(b) (…)

(c) (…)

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(da) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(db) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in conformity with Union law or Member State procedural law.

1b. Each supervisory authority shall have the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

Your Notes

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(ca) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(da) to order the controller to communicate a personal data breach to the data subject;

(e) to impose a temporary or definitive limitation including a ban on processing;

(f) to order the rectification, restriction or erasure of data pursuant to Articles 16, 17 and 17a and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;

(fa) (new) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Article 39 and 39a, or to order the certification body not to issue certification if the requirements for the certification are not or no longer met;

(g) to impose an administrative fine pursuant to Articles 79, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(h) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(i) (…)

(j) (…)

1c. Each supervisory authority shall have the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 34;

(aa) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(ab) to authorise processing referred to in Article 34(7a), if the law of the Member State requires such prior authorisation;

(ac) to issue an opinion and approve draft codes of conduct pursuant to Article 38(2);

(ad) to accredit certification bodies pursuant to Article 39a;

(ae) to issue certifications and approve criteria of certification in accordance with Article 39(2a);

(b) to adopt standard data protection clauses referred to in Article 26(2c) and in point (c) of Article 42(2);

(c) to authorise contractual clauses referred to in point (a) of Article 42(2a);

(ca) to authorise administrative agreements referred to in point (d) of Article 42(2a);

(d) to approve binding corporate rules pursuant to Article 43.

Your Notes

2. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.

3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

4. Each Member State may provide by law that its supervisory authority shall have additional powers than those referred to in paragraphs 1, 1b and 1c. These exercise of these powers shall not impair the effective functioning of the provisions of Chapter VII.

Article 54 - Activity Report

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of notified breaches and types of imposed sanctions. The report shall be transmitted to the national Parliament, the government and other authorities as designated by national law. It shall be made available to the public, the Commission and the European Data Protection Board.

Your Notes

Your Notes

SECTION 1 - CO-OPERATION

Article 54a - Cooperation between the lead supervisory authority and other concerned supervisory authorities

1. The lead supervisory authority shall cooperate with the other concerned supervisory authorities in accordance with this article in an endeavour to reach consensus. The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other.

1a. The lead supervisory authority may request at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

2. The lead supervisory authority shall, without delay communicate the relevant information on the matter to the other concerned supervisory authorities. It shall without delay submit a draft decision to the other concerned supervisory authorities for their opinion and take due account of their views.

3. Where any of the other concerned supervisory authorities within a period of four weeks after having been consulted in accordance with paragraph 2, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 57.

3a. Where the lead supervisory authority intends to follow the objection made, it shall submit to the other concerned supervisory authorities a revised draft decision for their opinion. This revised draft decision shall be subject to the procedure referred to in paragraph 3 within a period of two weeks.

4. Where none of the other concerned supervisory authorities has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 3 and 3a, the lead supervisory authority and the concerned supervisory authorities shall be deemed to be in agreement with this draft decision and shall be bound by it.

4a. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other concerned supervisory authorities and the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

4b. By derogation from paragraph 4a, where a complaint is dismissed or rejected, the supervisory authority to which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

4bb. Where the lead supervisory authority and the concerned supervisory authorities are in agreement to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint and notify it on that complainant and shall inform the controller or processor thereof.

4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a and 4bb, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other concerned supervisory authorities.

4d. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.

5. The lead supervisory authority and the other concerned supervisory authorities shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 55 - Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would be incompatible with the provisions of this Regulation or with Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request.

Your Notes

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1). In this case, the urgent need to act under Article 61(1) shall be presumed to be met and require an urgent binding decision from the European Data Protection Board pursuant to Article 61(2).

9. (…)

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 56 - Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff from other Member States' supervisory authorities are involved.

2. In cases where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member States are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations, as appropriate. The competent supervisory authority in accordance with Article 51a (1) or 51a(2c) shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in compliance with its own Member State law, and with the seconding supervisory authority’s authorisation, confer powers, including investigative powers on the seconding supervisory authority’s members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority’s members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law.

Your Notes

3a. Where, in accordance with paragraph 1, staff of a seconding supervisory authority are operating in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the persons entitled on their behalf.

3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State.

4. (…)

5. Where a joint operation is intended and a supervisory authority does not comply within one month with the obligation laid down in the second sentence of paragraph 2, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 51. In this case, the urgent need to act under Article 61(1) shall be presumed to be met and require an opinion or an urgent binding decision from the European Data Protection Board pursuant to Article 61(2).

6. (…)

SECTION 2 - CONSISTENCY

Article 57 - Consistency mechanism

1. In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall co-operate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this section.

Article 58 - Opinion by the European Data Protection Board

1. The European Data Protection Board shall issue an opinion whenever a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the European Data Protection Board, when it: c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2a); or

(ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or

(cb) aims at approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a; or

Your Notes

(d) aims at determining standard data protection clauses referred to in point (c) of Article 42(2) and paragraph (2c) of Article 26; or

(e) aims to authorising contractual clauses referred to in Article 42(2a(a)); or

(f) aims at approving binding corporate rules within the meaning of Article 43.

2. Any supervisory authority, the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

3. In the cases referred to in paragraphs 1 and 2, the European Data Protection Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. This opinion shall be adopted within eight weeks by simple majority of the members of the European Data Protection Board. This period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 6, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. (…)

5. Supervisory authorities and the Commission shall without undue delay electronically communicate to the European Data Protection Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other concerned supervisory authorities.

6. The chair of the European Data Protection Board shall without undue delay electronically inform:

(a) the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the European Data Protection Board shall, where necessary, provide translations of relevant information.

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

7. (…)

7a. Within the period referred to in paragraph 3 the competent supervisory authority shall not adopt its draft decision referred to in paragraph 1.

7b. (…)

8. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion, electronically communicate to the

Your Notes

chair of the European Data Protection Board whether it maintains or will amend its draft decision and, if any, the amended draft decision, using a standardised format.

9. Where the supervisory authority concerned informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph 1 of Article 58a shall apply.

Your Notes

Article 58a - Dispute Resolution by the European Data Protection Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the European Data Protection Board shall adopt a binding decision in the following cases:

(a) Where, in a case referred to in paragraph 3 of Article 54a, a supervisory authority concerned has expressed a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant and/or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of the Regulation;

(b) Where there are conflicting views on which of the concerned supervisory authorities is competent for the main establishment;

(d) Where a competent supervisory authority does not request the opinion of the European Data Protection Board in the cases mentioned in paragraph 1 of Article 58, or does not follow the opinion of the European Data Protection Board issued Article 58. In that case, any supervisory authority concerned or the Commission may communicate the matter to the European Data Protection Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the concerned supervisory authorities and binding on them.

3. In case the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. In case the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The concerned supervisory authorities shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. (…)

6. The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 to the concerned supervisory authorities. It shall inform the Commission thereof. The decision shall be published on the website of the European Data Protection Board without delay after the supervisory authority has notified the final decision referred to in paragraph 7.

7. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1, without undue delay and at the latest by one month after the European Data Protection Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged, shall inform the European Data Protection Board of the date when its final decision is notified respectively to the controller or the processor and the data subject. The final decision of the concerned supervisory authorities shall be adopted under the terms of Article 54a, paragraph 4a, 4b and

4bb. The final decision shall refer to the decision referred to in paragraph 1 and shall specify that the decision referred to in paragraph 1 will be published on the website of the European Data Protection Board in accordance with paragraph 6. The final decision shall attach the decision referred to in paragraph 1.

Your Notes

Article 59 - Opinion by the Commission (...)

Article 60 - Suspension of a draft measure (...)

Article 61 - Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 57, 58 and 58a or the procedure referred to in Article 54a, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the other concerned supervisory authorities, the European Data Protection Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the European Data Protection Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the European Data Protection Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from paragraph 3 of Article 58 and paragraph 2 of Article 58a, an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62 - Exchange of information

1. The Commission may adopt implementing acts of general scope for

(a) (…)

(b) (…)

(c) (…)

(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

2. (…)

3. (…)

Article 63 - Enforcement (...)

SECTION 3 - EUROPEAN DATA PROTECTION BOARD

Article 64 - European Data Protection Board

1a. The European Data Protection Board is hereby established as body of the Union and shall have legal personality.

1b. The European Data Protection Board shall be represented by its Chair.

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with the national law of that Member State.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board without voting right. The Commission shall designate a representative. The chair of the European Data Protection Board shall communicate to the Commission the activities of the European Data Protection Board.

5. In cases related to Article 58a, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices, and agencies which correspond in substance to those of this Regulation.

Article 65 - Independence

1. The European Data Protection Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 66 and 67.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Your Notes

Article 66 - Tasks of the European Data Protection Board

Your Notes

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(3) without prejudice to the tasks of national supervisory authorities;

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(aa) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(ab) (new) issue guidelines, recommendations, and best practices on procedures for deleting links, copies or replications of personal data from publicly available communication services as referred to in Article 17 paragraph 2;

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(ba) (new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 20(2);

(bb) (new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for establishing the data breaches and determining the undue delay referred to in paragraphs 1 and 2 of Article 31 and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(bc) (new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) as to the circumstances in which a personal data breach is likely to result in a high risk for the rights and freedoms of the individuals referred to in Article 32(1).

(bd) (new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for the purpose of further specifying the criteria and requirements for data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 43;

(be) (new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for the purpose of further specifying the criteria and requirements for the data transfers on the basis of Article 44(1);

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79;

(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and (ba); (ca0) issue guidelines, recommendations and best practices in accordance with point (b) of paragraph 1 for establishing common procedures for reporting by individuals of infringements of this Regulation pursuant to Article 49(2).

(ca) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;

(cb) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4 of Article 39;

(cd) specify the requirements mentioned in paragraph 3 of Article 39a with a view to the accreditation of certification bodies under Article 39;

(cda) give the Commission an opinion on the certification requirements referred to in paragraph 7 of Article 39a;

(cdb) give the Commission an opinion on the the icons referred to in paragraph 4b of Article 12;

(ce) give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in paragraph 2 and on matters submitted pursuant to paragraph 4 of Article 57;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(gb) issue opinions on codes of conduct drawn up at Union level pursuant to Article 38(4);

(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues dealt with in the consistency mechanism.

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

Your Notes

4. (…)

4a. The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

Article 67 - Reports

1. (…)

2. The European Data Protection Board shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1) as well as of the binding decisions referred to in paragraph 3 of Article 57.

Article 68 - Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The European Data Protection Board shall adopt its own rules of procedure by a two-third majority of its members and organise its own operational arrangements.

Article 69 - Chair

1. The European Data Protection Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 70 - Tasks of the chair

1. The chair shall have the following tasks:

(a) to convene the meetings of the European Data Protection Board and prepare its agenda;

(aa) to notify decisions adopted by the European Data Protection Board pursuant to Article 58a to the lead supervisory authority and the concerned supervisory authorities;

(b) to ensure the timely performance of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairs in its rules of procedure.

Your Notes

Article 71 - Secretariat

1. The European Data Protection Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

1a. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the European Data Protection Board.

1b. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

1c. Where appropriate, the European Data Protection Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation.

2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board.

3. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the European Data Protection Board;

(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;

(c) the use of electronic means for the internal and external communication;

(d) the translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection Board;

(f) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the European Data Protection Board.

Article 72 - Confidentiality

1. The discussions of the European Data Protection Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001.

3. (…)

Your Notes

Your Notes

Article 73 - Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringment if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation.
2. (…)
3. (…)
4. (…)
5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 74.

Article 74 - Right to a judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decisions of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority competent in accordance with Article 51 and Article 51a does not deal with a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged under Article 73.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

4. (…)
5. (…)

Article 75 - Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 73, each data subject shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non- compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of

the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

3. (…)

4. (…)

Your Notes

Article 76 - Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State, which is of non-profit making character, and whose statutory objectives are in the public interest and which is active in the field of the protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf and to exercise the right to receive compensation referred to in Article 77 on his or her behalf if provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1, independently of a data subject's mandate, shall have in such Member State the right to lodge a complaint with the supervisory authority competent in accordance with Article 73 and to exercise the rights referred to in Articles 74 and 75 if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with this Regulation.

3. (…)

4. (…)

5. (…)

Article 76a - Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 77 - Right to compensation and liability

1. Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in the processing shall be liable for the damage caused by the processing which is not in compliance with this Regulation. A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempted from liability in accordance with paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor or a controller and a processor are involved in the same processing and, where they are, in accordance with paragraphs 2 and 3, responsible for any damage caused by the processing, each controller or processor shall be held liable for the entire damage, in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under national law of the Member State referred to in paragraph 2 of Article 75.

Article 78 - Penalties (…)

Article 79 - General conditions for imposing administrative fines

1a. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 3 (new), 3a (new), 3aa (new) shall in each individual case be effective, proportionate and dissuasive.

2. (…)

2a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (fa) and (h) of paragraph 1b of Article 53. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) (…)

(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;

(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;

Your Notes

(f) any relevant previous infringements by the controller or processor;

(g) (new) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(ga) (new) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in paragraph 1b of Article 53, have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with these measures;

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;

(k) (…)

(m) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

2b. If a controller or processor intentionally or negligently, for the same or linked processing operations, violates several provisions of this Regulation, the total amount of the fine may not exceed the amount specified for the gravest violation.

3. (…)

3 (new). Infringments of the following provisions shall, in acccordance with paragraph 2a, be subject to administrative fines up to 10 000 000 EUR, or in case of an undertaking, up to 2% of the total worlwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 10, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39 and 39a;

(aa) the obligations of the certification body pursuant to Articles 39 and 39a;

(ab) the obligations of the monitoring body pursuant to Article 38a(4);

3a (new). Infringments of the following provisions shall, in acccordance with paragraph 2a, be subject to administrative fines up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worlwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12-20;

(ba) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 40-44;

(bb) any obligations pursuant to Member State laws adopted unter Chapter IX;

Your Notes

(c) non-compliance with an order or a temporary or definite limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 53 (1b) or does not provide access in violation of Article 53(1).

3aa (new). Non-compliance with an order by the supervisory authority as referred to in Article 53(1b) shall, in acccordance with paragraph 2a, be subject to administrative fines up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worlwide annual turnover of the preceding financial year, whichever is higher:

3b. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 53(1b), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

4. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.

5. Where the legal system of the Member State does not provide for administrative fines, Article 79 may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that these legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. These Member States shall notify to the Commission those provisions of their laws by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

6. (…)

7. (…)

Article 79b - Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 79, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. (…)

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Your Notes

Your Notes

Article 80 - Processing of personal data and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 80a - Processing of personal data and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 80aa - Processing of personal data and reuse of public sector information (...)

Article 80b - Processing of national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In this case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 81 - Processing of personal data for health - related purposes

(…)

Article 81a - Processing of genetic data

(…)

Article 82 - Processing in the employment context

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge

of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. These rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of data within a group of undertakings or group of entreprises and monitoring systems at the work place.

2a. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. (…)

Your Notes

Article 83 - Safeguards and derogations for the processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

1. Processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes, shall be subject to in accordance with this Regulation appropriate safeguards for the rights and freedoms of the data subject. These safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure the respect of the principle of data minimisation. These measures may include pseudonymisation, as long as these purposes can be fulfilled in this manner. Whenever these purposes can be fulfilled by further processing of data which does not permit or not any longer permit the identification of data subjects these purposes shall be fulfilled in this manner.

2. Where personal data are processed for scientific and historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 17a and 19 subject to the conditions and safeguards referred to in paragraph 1 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 these purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 17a, 17b, 18 and 19 subject to the conditions and safeguards referred to in paragraph 1 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 these purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to the processing for the purposes referred to in those paragraphs.

Article 84 - Obligations of secrecy

1. Member States may adopt specific rules to set out the powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects under Union or Member State law or rules established by national competent bodies to an obligation of professional secrecy or other

equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 85 - Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1, shall be subject to the control of an independent supervisory authority which may be specific, provided that fulfils the conditions laid down in Chapter VI of this Regulation.

Your Notes

Your Notes

Article 86 - Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 12(4c) and Article 39a(7) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.
3. The delegation of power referred to in Article 12(4c) and Article 39a(7) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 12(4c) and Article 39a(7) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or the Council.

Article 87 - Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

Your Notes

Article 88 - Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed on the date specified in Article 91(2).

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 89 - Relationship to Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 89b - Relationship to previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Union law applicable prior to the entry into force of this Regulation, shall remain in force until amended, replaced or revoked.

Article 90 - Evaluation

1. The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals.

2. In the context of these evaluations the Commission shall examine, in particular, the application and functioning of the provisions of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to article 41(3) and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on Co-operation and Consistency.

2a. For the purpose referred to in paragraph 1, the Commission may request information from Member States and supervisory authorities.

2b. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, the Council, as well as other relevant bodies or sources.

3. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The reports shall be made public.

4. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, in particular taking into account of developments in information technology and in the lightof the state of progress in the information society.

Article 90a (new) - Review of other EU data protection instruments

The Commission shall, if appropriate, submit legislative proposals with a view to amending other EU legal instruments on the protection of personal data, in order to ensure uniform and consistent protection of individuals with regard to the processing of personal data. This shall in particular concern the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 91 - Entry into force and application

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

2. It shall apply from [two years from the date referred to in paragraph 1]. * * OJ: insert the date. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

Your Notes