National accreditation body

General Data Protection Regulation

Obligations

Principle of lawfulness, fairness and transparency

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/a

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

Purpose limitation principle

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/b

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

Data minimization principle

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/c

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

Principle of accuracy

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/d

Personal data shall be 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');

Storage limitation principle

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/e

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

Principle of integrity and confidentiality

(In role Controller) (In role Processor)

Chapter II, Article 5, Paragraph 1/f

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

Principle of accountability

(In role Controller)

Chapter II, Article 5, Paragraph 2

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

Processing for a purpose other than that for which the personal data have been collected originally

(In role Controller)

Chapter II, Article 6, Paragraph 4

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Obligation to demonstrate the consent for processing the personal data

(In role Controller)

Chapter II, Article 7, Paragraph 1

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

Obligations of the controller on context of the child when processing the personal data

(In role Controller)

Chapter II, Article 8, Paragraph 2

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.

Prohibition of processing the special categories of personal data

(In role Controller) (In role Processor)

Chapter II, Article 9, Paragraph 1

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

Reasons for derogating the exercise of the Articles 15 – 20

(In role Controller)

Chapter II, Article 11, Paragraph 2

Where, in cases referred to in paragraph 1 of this Article, 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 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Measures of the controller in terms of providing the information to data subjects

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 1

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Facilitating the data subject rights

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 2

The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(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 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Providing the information on action taken on a request under Articles 15 to 22 to the data subject

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 3

The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Obligations of the controller in case when the data subject request is unadopted

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 4

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 with a supervisory authority and seeking a judicial remedy.

Information provided to the data subject when personal data has been acquired from a data subject

(In role Controller)

Chapter III, Section 2, Article 13, Paragraph 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 all of the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact 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 the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Additional information provided to the data subject when personal data has been acquired from a data subject

(In role Controller)

Chapter III, Section 2, Article 13, Paragraph 2

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 that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) 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;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject..

Information provided to the data subject when controller intends to further process the personal data for a purpose other than that for which the personal data were collected

(In role Controller)

Chapter III, Section 2, Article 13, Paragraph 3

Where the controller intends to further process the personal data for a purpose other than that for which the personal 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 2.

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

(In role Controller)

Chapter III, Section 2, Article 14, Paragraph 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, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) the categories of personal data concerned;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, that the 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 the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

Some additional information provided where personal data have not been obtained from the data subject

(In role Controller)

Chapter III, Section 2, Article 14, Paragraph 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:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) 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) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d) where 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;
(e) the right to lodge a complaint with a supervisory authority;
(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Principles of providing the information in terms of the Article 14, paragraph 1 and 2 of the regulation

(In role Controller)

Chapter III, Section 2, Article 14, Paragraph 3

The controller shall provide the information referred to in paragraphs 1 and 2:
(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Providing the information where the controller intends to process the personal data for a purpose other than that for which the personal data were obtained

(In role Controller)

Chapter III, Section 2, Article 14, Paragraph 4

Where the controller intends to further process the personal data for a purpose other than that for which the personal 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.

Obligation to provide a copy of the personal data which are being processed

(In role Controller)

Chapter III, Section 2, Article 15, Paragraph 3

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 by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Obligations of the controller after the right to be forgotten has been applied

(In role Controller)

Chapter III, Section 3, Article 17, Paragraph 2

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal 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 personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Information duty of the controller in context of the personal data processing limitation

(In role Controller)

Chapter III, Section 3, Article 18, Paragraph 3

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

Information obligation of the controller towards the recipients

(In role Controller)

Chapter III, Section 3, Article 19

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal 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 it.

Right of the data subject to object the processing of personal data

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 1

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the 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.

Prohibition of the personal data processing after the Article 21, paragraph 2 has been applied

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 3

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

Obligation of the controller to inform the data subject about the to object

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 4

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.

Proceedings of the controller in case of the Article 22, paragraph 2, points a) – c) application

(In role Controller)

Chapter III, Section 4, Article 22, Paragraph 3

In the cases referred to in points (a) and (c) of paragraph 2, 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.

Responsibilities of the controller relating to the personal data processing

(In role Controller)

Chapter IV, Section 1, Article 24, Paragraph 1

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

Implementation of an appropriate data protection policies by the controller

(In role Controller)

Chapter IV, Section 1, Article 24, Paragraph 2

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

Implementation of the appropriate technical and organisational measures

(In role Controller)

Chapter IV, Section 1, Article 25, Paragraph 1

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the 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 manner 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.

Processing of the personal data “by default”

(In role Controller)

Chapter IV, Section 1, Article 25, Paragraph 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Personal data processing by the joint controllers

(In role Controller) (In role Joint Controller)

Chapter IV, Section 1, Article 26, Paragraph 1

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with 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 13 and 14, 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 contact point for data subjects.

Respective roles and relationships of the joint controllers vis-à-vis the data subjects

(In role Controller) (In role Joint Controller)

Chapter IV, Section 1, Article 26, Paragraph 2

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

Designating the place of activity of the controller, that is settled outside the EU

(Delegated Representative of the Controller)

Chapter IV, Section 1, Article 27, Paragraph 3

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

Guaranties of the processor for implementing the adequate protective measurements

(In role Controller)

Chapter IV, Section 1, Article 28, Paragraph 1

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

Conditions for engaging the other processor to the data processing

(In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 2

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

Designation of the identical scope of the responsibilities for the other processor

(In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 4

Where a processor engages 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 3 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 appropriate technical and organisational measures in such a manner 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.

Contract or any other legal document in terms of the Article 28, paragraphs 3 and 4

(In role Controller) (In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 9

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

Consequences of misconducting the purposes and instruments in the process of personal data processing by the processor

(In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 10

Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Obligation of the processor to comply with the instructions of the controller

(In role Processor)

Chapter IV, Section 1, Article 29

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 those data except on instructions from the controller, unless required to do so by Union or Member State law.

Mandatory scope of the processing activities record

(In role Controller) (Delegated Representative of the Controller)

Chapter IV, Section 1, Article 30, Paragraph 1

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

A record of all the processing activities categories, that are carried on behalf of a controller

(In role Processor) (Delegated Representative of the Processor)

Chapter IV, Section 1, Article 30, Paragraph 2

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of 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, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Form of the records according to Article 30, paragraphs 1 and 2

(In role Controller) (In role Processor)

Chapter IV, Section 1, Article 30, Paragraph 3

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

Making the records available to the supervisory authority if needed

(In role Controller) (In role Processor) (Delegated Representative of the Controller) (Delegated Representative of the Processor)

Chapter IV, Section 1, Article 30, Paragraph 4

The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

Cooperation with the supervisory authority

(In role Controller) (In role Processor) (Delegated Representative of the Controller) (Delegated Representative of the Processor)

Chapter IV, Section 1, Article 31

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Implementation of the appropriate technical and organisational measures

(In role Controller) (In role Processor)

Chapter IV, Section 2, Article 32, Paragraph 1

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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 processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Ensuring the activities compliance of any natural person, acting under the authority of controller or processor

(In role Controller) (In role Processor)

Chapter IV, Section 2, Article 32, Paragraph 4

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

Period for declaring the personal data breach

(In role Controller)

Chapter IV, Section 2, Article 33, Paragraph 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 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Notification the data breach to the controller

(In role Processor)

Chapter IV, Section 2, Article 33, Paragraph 2

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

The minimal content of the personal data breach notification

(In role Controller)

Chapter IV, Section 2, Article 33, Paragraph 3

The notification referred to in paragraph 1 shall at least:
(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Documentary measures relating to the personal data breach

(In role Controller)

Chapter IV, Section 2, Article 33, Paragraph 5

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

Communication the personal data breach to the data subject

(In role Controller)

Chapter IV, Section 2, Article 34, Paragraph 1

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

Personal data processing that require the DPIA – general provision

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 1

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the 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.

Cooperation between the controller and data protection officer

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 2

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

Gathering the opinions of data subjects or their representatives

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 9

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 processing operations.

Situation where the DPIA might be necessary

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 11

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

Situations that require the prior consultations with the supervisory authority

(In role Controller)

Chapter IV, Section 3, Article 36, Paragraph 1

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Information provided for the supervisory authority by the controller

(In role Controller)

Chapter IV, Section 3, Article 36, Paragraph 3

When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:
(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within 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 35; and
(f) any other information requested by the supervisory authority.

Compulsory designation of the data protection officer (DPO)

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 37, Paragraph 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;
(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 personal data relating to criminal convictions and offences referred to in Article 10.

Publishing the data of the designated data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 37, Paragraph 7

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

Responsibility of the controller and processor in context of the Data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 38, Paragraph 1

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

Providing the support for the data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 38, Paragraph 2

The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

Organizational status of the Data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 38, Paragraph 3

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

The Data protection officer and it´s other tasks and duties

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 38, Paragraph 6

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

Common certification and the European Data Protection Seal

(In role Certification body)

Chapter IV, Section 4, Article 42, Paragraph 5

A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

Providing the information and access, that are essential for the certification procedure

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 42, Paragraph 6

The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

Issuing the certification

(In role Certification body)

Chapter IV, Section 4, Article 43, Paragraph 1

Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:
(a) the supervisory authority which is competent pursuant to Article 55 or 56;
(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

Validity of the accreditation and it´s prolongation

(In role Certification body)

Chapter IV, Section 4, Article 43, Paragraph 4

The certification bodies 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 shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

Information obligation of the certification subjects

(In role Certification body)

Chapter IV, Section 4, Article 43, Paragraph 5

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

Revocation of the accreditation

Chapter IV, Section 4, Article 43, Paragraph 7

Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

Documentation of the assessment and suitable safeguards

(In role Controller) (In role Processor)

Chapter V, Article 49, Paragraph 6

The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Obligations of the controller (or processor) after the decision has been published

(In role Controller) (In role Processor)

Chapter VII, Section 1, Article 60, Paragraph 10

After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards 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 supervisory authorities concerned.

Joint liability in context of the personal data processing

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 4

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

Appropriate safeguards related to the rights and freedoms of the data subject

(In role Controller) (In role Processor)

Chapter IX, Article 89, Paragraph 1

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

Rights

Exemption from the obligation to maintain, acquire or process additional information in order to identify the data subject

(In role Controller)

Chapter II, Article 11, Paragraph 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.

Rights of the controller in case of the inappropriate requests from the data subject

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 5

Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 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 either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Additional information claims from the controller

(In role Controller)

Chapter III, Section 1, Article 12, Paragraph 6

Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Possibilities of declaring the obligations fulfilment

(In role Controller)

Chapter IV, Section 1, Article 24, Paragraph 3

Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Approved certification mechanism pursuant to Article 42

(In role Controller)

Chapter IV, Section 1, Article 25, Paragraph 3

An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Conditions for engaging the other processor to the data processing

(In role Controller)

Chapter IV, Section 1, Article 28, Paragraph 2

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

Certification mechanism as referred to in Article 42

(In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 5

Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

Adherence to an approved code of conduct as referred to in Article 40

(In role Controller) (In role Processor)

Chapter IV, Section 2, Article 32, Paragraph 3

Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Additional information relating to the personal data breach notification

(In role Controller) (In role Processor)

Chapter IV, Section 2, Article 33, Paragraph 4

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

Situation where the notification obligation shall not apply

(In role Controller)

Chapter IV, Section 2, Article 34, Paragraph 3

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Optional designation of the Data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 37, Paragraph 4

In cases other than those referred to in paragraph 1, the controller or processor or Associations and other bodies representing 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.

Personal data transfer in case of the absence of the decision based on the Article 45(3)

(In role Controller) (In role Processor)

Chapter V, Article 46, Paragraph 1

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

Right to an effective judicial remedy against a supervisory authority

(In role Legal person)

Chapter VIII, Article 78, Paragraph 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 decision of a supervisory authority concerning them.

Compensation for the damage suffered

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 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.

Indirect obligations

Right of the data subject to obtain a confirmation of the personal data processing from the controller

(In role Controller)

Chapter III, Section 2, Article 15, Paragraph 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 that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with 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 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right to be informed of appropriate safeguards pursuant to Article 46 relating to the transfer

(In role Controller)

Chapter III, Section 2, Article 15, Paragraph 2

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

Right to rectification

(In role Controller)

Chapter III, Section 3, Article 16

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

Reason for eligibility of the data subject to exercise the right to be forgotten

(In role Controller)

Chapter III, Section 3, Article 17, Paragraph 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 personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal 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 personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Restraining the personal data processing

(In role Controller)

Chapter III, Section 3, Article 18, Paragraph 1

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the 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;
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data s

Right of the data subject to personal data portability

(In role Controller)

Chapter III, Section 3, Article 20, Paragraph 1

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, 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 personal 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.

Portability of the personal data from one controller to another controller

(In role Controller)

Chapter III, Section 3, Article 20, Paragraph 2

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

Right of the data subject to object the processing of personal data

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 1

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the 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.

Right of the data subject to object the personal data processing related to the marketing purposes

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 2

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to 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.

Right to object the personal data processing for the purposes of the scientific, historical or statistical reasons

(In role Controller)

Chapter III, Section 4, Article 21, Paragraph 6

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(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.

Right not to be subject to a decision based solely on the automated processing

(In role Controller)

Chapter III, Section 4, Article 22, Paragraph 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.

Exercising the rights of the data subject against each of the controllers

(In role Controller)

Chapter IV, Section 1, Article 26, Paragraph 3

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.

Competencies of the supervisory authority, in relation to the personal data breach notification

(In role Controller)

Chapter IV, Section 2, Article 34, Paragraph 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 personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Investigative powers of the supervisory authority

(In role Controller) (In role Processor) (Delegated Representative of the Controller) (Delegated Representative of the Processor)

Chapter VI, Section 2, Article 58, Paragraph 1

Each supervisory authority shall have all of 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;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Corrective powers of the supervisory authority

(In role Controller) (In role Processor)

Chapter VI, Section 2, Article 58, Paragraph 2

Each supervisory authority shall have all of 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;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) 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;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Compensation for the material or non-material damage as a result of an infringement of this Regulation

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 1

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

Special provisions in context of the responsibility for the damage in terms of the Article 82, paragraph 1

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 2

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

Compensation for the damage suffered

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 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.

Indirect rights

Information obligation of the controller towards the recipients

(In role Recipient)

Chapter III, Section 3, Article 19

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal 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 it.

Notification the data breach to the controller

(In role Controller)

Chapter IV, Section 2, Article 33, Paragraph 2

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

List of processing operations which require an obligatory data protection impact assessment

(In role Controller) (In role Processor)

Chapter IV, Section 3, Article 35, Paragraph 4

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 Board referred to in Article 68.

Competency of the supervisory authority in case of the specific situations

(In role Controller) (In role Processor)

Chapter IV, Section 3, Article 36, Paragraph 2

Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

Responsibility of the data protection officer

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 39, Paragraph 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 carry out processing 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 processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Support in working out the codes of conduct

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 40, Paragraph 1

The Member States, the supervisory authorities, the 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 processing sectors and the specific needs of micro, small and medium-sized enterprises.

Providing the information and access, that are essential for the certification procedure

(In role Certification body)

Chapter IV, Section 4, Article 42, Paragraph 6

The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

The notification obligation of the lead supervisory authority in case of the submitted appeal

(In role Controller) (In role Processor)

Chapter VII, Section 1, Article 60, Paragraph 7

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 supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

The notification obligation of the lead supervisory authority in case of the rejection of the submitted appeal

(In role Controller)

Chapter VII, Section 1, Article 60, Paragraph 8

By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

The proceeding of the lead supervisory authority and other supervisory authorities in case of the partial rejection of the submitted appeal

(In role Controller) (In role Processor)

Chapter VII, Section 1, Article 60, Paragraph 9

Where the lead supervisory authority and the supervisory authorities concerned agree 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, shall 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 shall notify it to that complainant and shall inform the controller or processor thereof.

Scope of the Board activities and responsibilities

(In role Controller) (In role Processor)

Chapter VII, Section 3, Article 70, Paragraph 1

The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:
(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;
(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
(e) examine, on its own initiative, 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;
(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).
(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal 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 47;
(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);
(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;
(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);
(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);
(n) 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 40 and 42;
(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;
(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);
(r) provide the Commission with an opinion on the icons referred to in Article 12(7);
(s) rovide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.
(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;
(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;
(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and
(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

Definitions

Territorial scope for the EU subjects

(In role Controller in the EU) (In role Processor in the EU)

Chapter I, Article 3, Paragraph 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.

Controller

(In role Controller)

Chapter I, Article 4, Paragraph 7

For the purposes of this Regulation:
'controller' means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Processor

(In role Processor)

Chapter I, Article 4, Paragraph 8

For the purposes of this Regulation:
'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient

(In role Recipient)

Chapter I, Article 4, Paragraph 9

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

Third party

(In role Third party)

Chapter I, Article 4, Paragraph 10

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

Compliance with a legal obligation

(In role Controller)

Chapter II, Article 6, Paragraph 1/c

Processing shall be lawful only if and to the extent that at least one of the following applies: (c) processing is necessary for compliance with a legal obligation to which the controller is subject

Performance of a task carried out in the public interest

(In role Controller)

Chapter II, Article 6, Paragraph 1/e

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

Purposes of the legitimate interests pursued by the controller or by a third party

(In role Controller) (In role Third party)

Chapter II, Article 6, Paragraph 1/f

Processing shall be lawful only if and to the extent that at least one of the following applies:
(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.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Exclusions from the prohibition of processing the special categories of personal data

(In role Controller)

Chapter II, Article 9, Paragraph 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 or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(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 or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit 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 personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(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;
(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 or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) 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 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;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(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.

Exemptions from application the obligation of the controller to provide information in terms of the Article 14, paragraphs 1 – 4

(In role Controller)

Chapter III, Article 14, Section 2, Paragraph 5

Paragraphs 1 to 4 shall not apply where and insofar as:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible

or seriously impair the achievement of the objectives of that processing. 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;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Limitation of the negative implications in context of the other subjects' rights

(In role Controller)

Chapter III, Section 2, Article 15, Paragraph 4

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

Exemptions from the application of Article 17, paragraph 1 and 2

(In role Controller)

Chapter III, Section 3, Article 17, Paragraph 3

Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing 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 points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(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 that processing; or
(e) for the establishment, exercise or defence of legal claims.

Processing the personal data after the right to restriction of processing has been applied

(In role Controller) (In role Legal person)

Chapter III, Section 3, Article 18, Paragraph 2

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

Limitation of the right to obtain the personal data

(In role Controller)

Chapter III, Section 3, Article 20, Paragraph 3

The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Limitation of the negative implications relating to other subjects' rights

(In role Controller)

Chapter III, Section 3, Article 20, Paragraph 4

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

Restrictions in application of the Article 22, paragraph 1

(In role Controller)

Chapter III, Section 4, Article 22, Paragraph 2

Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised 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.

Minimum scope of the individual provisions in terms of the Article 23, paragraph 1 of the regulation

(In role Controller) (In role Processor)

Chapter III, Section 5, Article 23, Paragraph 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 to the rights and freedoms of data subjects; and
(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Legal instruments of the remedies against the controller or processor

(Delegated Representative of the Controller) (Delegated Representative of the Processor)

Chapter IV, Section 1, Article 27, Paragraph 5

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

Minimal scope of the contract essentials between the Controller and Processor

(In role Controller) (In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 3

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
a) processes 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, unless that law prohibits such information on important grounds of public interest;
b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) takes all measures required pursuant to Article 32;
d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
taking into account the nature of the processing, assists 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;
d) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
f) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
g) makes 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.
With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

Basic Standard contract clauses between the Controller and Processor

(In role Controller) (In role Processor)

Chapter IV, Section 1, Article 28, Paragraph 6

Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

Exemption from the obligations listed in the Article 30, paragraph 1 and 2

(In role Enterprise or an organisation employing fewer than 250 persons)

Chapter IV, Section 1, Article 30, Paragraph 5

The obligations referred to in paragraphs 1 and 2 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 to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Assessing the appropriate level of the security account

(In role Controller) (In role Processor)

Chapter IV, Section 2, Article 32, Paragraph 2

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

Notification method in context of the Article 34, paragraph 1 of the regulation

(In role Controller)

Chapter IV, Section 2, Article 34, Paragraph 2

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

Processing that requires the obligatory DPIA

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 3

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

Minimal content of the DPIA

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 7

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

Assessing the impact of the processing performed by such controllers or processors

(In role Controller) (In role Processor)

Chapter IV, Section 3, Article 35, Paragraph 8

Compliance with approved codes of conduct referred to in Article 40 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.

Situations where the DPIA need not to be done

(In role Controller)

Chapter IV, Section 3, Article 35, Paragraph 10

Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

Supervisory authority consultation relating to social policy and public health policy

(In role Controller)

Chapter IV, Section 3, Article 36, Paragraph 5

Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Monitoring the compliance of the codes of conduct

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 40, Paragraph 4

A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) 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 supervisory authorities competent pursuant to Article 55 or 56.

Responsibility of the Controller and Processor relating to the certification process

(In role Controller) (In role Processor)

Chapter IV, Section 4, Article 42, Paragraph 4

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 authorities which are competent pursuant to Article 55 or 56.

Validity of the certificate and it´s prolongation

(In role Certification body) (In role Controller) (In role Processor)

Chapter IV, Section 4, Article 42, Paragraph 7

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

Accreditation conditions in relation to the certification subjects

(In role Certification body) (In role Controller) (In role Processor)

Chapter IV, Section 4, Article 43, Paragraph 2

Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:
(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
(d) established procedures and structures to handle 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 those procedures and structures transparent to data subjects and the public; and
(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

Implementation criteria of the certification subjects accreditation process

(In role Certification body)

Chapter IV, Section 4, Article 43, Paragraph 3

The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

Basic conditions for the personal data transfer

(In role Controller) (In role Processor)

Chapter V, Article 44

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of 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 natural persons guaranteed by this Regulation is not undermined.

Possibilities of setting the appropriate safeguards up

(In role Controller) (In role Processor)

Chapter V, Article 46, Paragraph 2

The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e) an approved code of conduct pursuant to Article 40 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
(f) an approved certification mechanism pursuant to Article 42 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..

Priority forms and approaches of the appropriate safeguards based on the Article 46, paragraph 1

(In role Controller) (In role Processor) (In role Recipient)

Chapter V, Article 46, Paragraph 3

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 personal data in the third country or international organisation; or
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and

effective data subject rights.

Minimal essential content of the binding corporate rules

(In role Controller) (In role Processor)

Chapter V, Article 47, Paragraph 2

The binding corporate rules referred to in paragraph 1 shall specify at least:
(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity 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 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 processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, 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 shall be exempt from that liability, in whole or in part, only if it proves 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 13 and 14;
(h) he tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
(i) the complaint procedures;
(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity 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 to in point (h) and to the board of the controlling undertaking of Group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity 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
(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Mutual legal assistance between the requesting third country and the Union or a Member State

(In role Controller) (In role Processor)

Chapter V, Article 48

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.

Conditions for the personal data transfer in case of an appropriate safeguards decision absence

(In role Controller) (In role Legal person) (In role Processor)

Chapter V, Article 49, Paragraph 1

In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(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 by Union or Member State law for consultation are fulfilled in the particular case.
Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph 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, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

Specifications to the personal data transfer in context of the Article 49, paragraph 1

(In role Persons having a legitimate interest) (In role Recipient)

Chapter V, Article 49, Paragraph 2

A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

The lead supervisory authority in context of the cross-border processing

(In role Controller) (In role Processor)

Chapter VI, Section 2, Article 56, Paragraph 6

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

Access to documents of the Board

(In role Third party)

Chapter VII, Section 3, Article 76, Paragraph 2

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

The local competency of the judicial authorities for submitting the proceeding against the controller or processor

(In role Controller) (In role Processor)

Chapter VIII, Article 79, Paragraph 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.

Circumstances that are excluding the responsibility of the controller or processor for the damage

(In role Controller) (In role Processor)

Chapter VIII, Article 82, Paragraph 3

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

Restrictions in the exemptions based on the Article 89, paragraph 2 and 3

(In role Controller) (In role Processor)

Chapter IX, Article 89, Paragraph 4

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