Authorised subject

General Data Protection Regulation

Obligations

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

(Delegated Person acting under the authority of the controller or of the 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.

The confidentiality obligation of the Data protection officer

(In role Data protection officer)

Chapter IV, Section 4, Article 38, Paragraph 5

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

Responsibility of the data protection officer

(In role Data protection officer)

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.

Some other tasks of the Data protection officer

(In role Data protection officer)

Chapter IV, Section 4, Article 39, Paragraph 2

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

Assessment of the code of conduct by the supervisory authority

(Delegated Associations and other bodies representing Controllers or Processors)

Chapter IV, Section 4, Article 40, Paragraph 5

Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

Measurements taken in the situations when the code of conduct id breached by the Controller or Processor

(In role Accredited body which has an appropriate level of expertise in relation to the subject-matter of the code of conduct)

Chapter IV, Section 4, Article 41, Paragraph 4

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

Rights

Optional designation of the Data protection officer

(Delegated Associations and other bodies representing Controllers or Processors)

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.

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

(In role Data protection officer)

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.

Codes of conduct

(Delegated Associations and other bodies representing Controllers or Processors)

Chapter IV, Section 4, Article 40, Paragraph 2

Associations and other bodies representing Controllers or Processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
(a) fair and transparent processing;
(b) the legitimate interests pursued by controllers in specific contexts;
(c) the collection of personal data;
(d) the pseudonymisation of personal data;
(e) the information provided to the public and to data subjects;
(f) the exercise of the rights of data subjects;
(g) the information provided to, and the protection of, children, and the manner in which the content of the holders of parental responsibility over children is to be obtained;
(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
(j) the transfer of personal data to third countries or international organisations; or
(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

Monitoring the compliance with a code of conduct by the designated subject

(In role Accredited body which has an appropriate level of expertise in relation to the subject-matter of the code of conduct)

Chapter IV, Section 4, Article 41, Paragraph 1

Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

Basic criteria for an accreditation of a designated subject

(In role Accredited body which has an appropriate level of expertise in relation to the subject-matter of the code of conduct)

Chapter IV, Section 4, Article 41, Paragraph 2

A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:
(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

Indirect rights

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

(In role Data protection officer)

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 Data protection officer)

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 Data protection officer)

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 free – of -charge principle of performing the supervisory authority tasks

(In role Data protection officer)

Chapter VI, Section 2, Article 57, Paragraph 3

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

Definitions

Provisions regarding the processing of special categories of personal data in terms of the Article 9, paragraph 2, point h)

(In role Person subjected to an obligation of secrecy)

Chapter II, Article 9, Paragraph 3

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

Processing of personal data relating to criminal convictions and offences

(In role Official authority)

Chapter II, Article 10

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

Basic requirements for the Data protection officer job position

(In role Data protection officer)

Chapter IV, Section 4, Article 37, Paragraph 5

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

Appointing the employee to the position of the Data protection officer

(In role Data protection officer)

Chapter IV, Section 4, Article 37, Paragraph 6

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

Minimal essential content of the binding corporate rules

(In role Data protection officer)

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.