

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 19

Obligations of the controller

1 Member States shall provide for the controller, 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, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

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

Article 20

Data protection by design and by default

1 Member States shall provide for the controller, 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, both at the time of the determination of the means for processing and at the time of the processing itself, to 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 Directive and protect the rights of data subjects.

2 Member States shall provide for the controller to implement appropriate technical and organisational measures 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

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

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.

Article 21

Joint controllers

1 Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, 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 shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

2 Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

Article 22

Processor

1 Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

2 Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by 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.

3 Member States shall provide for the processing by a processor to 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 acts only on instructions from the controller;
- 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 assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
- d at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- e makes available to the controller all information necessary to demonstrate compliance with this Article;

f complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

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

5 If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

Article 23

Processing under the authority of the controller or processor

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

Article 24

Records of processing activities

1 Member States shall provide for controllers to maintain a record of all categories of processing activities under their 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 and the data protection officer;
- b the purposes of the processing;
- c the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- d a description of the categories of data subject and of the categories of personal data;
- e where applicable, the use of profiling;
- f where applicable, the categories of transfers of personal data to a third country or an international organisation;
- g an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;
- h where possible, the envisaged time limits for erasure of the different categories of personal data;
- i where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

2 Member States shall provide for each processor to 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, of each controller on behalf of which the processor is acting and, where applicable, 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 where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;
- d where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

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

The controller and the processor shall make those records available to the supervisory authority on request.

Article 25

Logging

1 Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2 The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

3 The controller and the processor shall make the logs available to the supervisory authority on request.

Article 26

Cooperation with the supervisory authority

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

Article 27

Data protection impact assessment

1 Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2 The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 28

Prior consultation of the supervisory authority

- 1 Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:
 - a a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
 - b the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.
- 2 Member States shall provide for the supervisory authority to be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing.
- 3 Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.
- 4 Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.
- 5 Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, 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.