

► **B** 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

(OJ L 119, 4.5.2016, p. 89)

Corrected by:

► **C1** Corrigendum, OJ L 127, 23.5.2018, p. 6 (2016/680)



**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 I

General provisions

Article 1

Subject-matter and objectives

1. This Directive lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security.
2. In accordance with this Directive, Member States shall:
 - (a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and
 - (b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

Article 2

Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).
2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
3. This Directive does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;

▼B

- (b) by the Union institutions, bodies, offices and agencies.

*Article 3***Definitions**

For the purposes of this Directive:

- (1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (5) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- (7) ‘competent authority’ means:
 - (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

▼B

- (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (8) ‘controller’ means the competent authority 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;
- (9) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (10) ‘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 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;
- (11) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (12) ‘genetic data’ means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (13) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (14) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (15) ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 41;
- (16) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

▼ B*CHAPTER II**Principles**Article 4***Principles relating to processing of personal data**

1. Member States shall provide for personal data to be:
 - (a) processed lawfully and fairly;
 - (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
 - (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
 - (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.
3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.
4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

▼B*Article 5***Time-limits for storage and review**

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

*Article 6***Distinction between different categories of data subject**

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

- (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
- (b) persons convicted of a criminal offence;
- (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
- (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

*Article 7***Distinction between personal data and verification of quality of personal data**

1. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.

2. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

3. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

▼B*Article 8***Lawfulness of processing**

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.
2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

*Article 9***Specific processing conditions**

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.
2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.
3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.
4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

*Article 10***Processing of special categories of personal data**

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

▼B

concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

- (a) where authorised by Union or Member State law;
- (b) to protect the vital interests of the data subject or of another natural person; or
- (c) where such processing relates to data which are manifestly made public by the data subject.

*Article 11***Automated individual decision-making**

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

*CHAPTER III****Rights of the data subject****Article 12***Communication and modalities for exercising the rights of the data subject**

1. Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.

▼ B

3. Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.

4. Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to 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.

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

*Article 13***Information to be made available or given to the data subject**

1. Member States shall provide for the controller to make available to the data subject at least the following information:

- (a) the identity and the contact details of the controller;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended;
- (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;
- (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

- (a) the legal basis for the processing;
- (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

▼B

- (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;
- (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

*Article 14***Right of access by the data subject**

Subject to Article 15, Member States shall provide for the right of the data subject 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 and legal basis for the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

▼B

- (f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;
- (g) communication of the personal data undergoing processing and of any available information as to their origin.

*Article 15***Limitations to the right of access**

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

*Article 16***Right to rectification or erasure of personal data and restriction of processing**

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

▼B

2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3. Instead of erasure, the controller shall restrict processing where:

- (a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or
- (b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

5. Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

6. Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, provide for the controller to notify the recipients and that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

▼B*Article 17***Exercise of rights by the data subject and verification by the supervisory authority**

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

*Article 18***Rights of the data subject in criminal investigations and proceedings**

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

*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.

▼B*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 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

▼B

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.

▼ B*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;

▼B

- (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).
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.

▼B

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.

▼B

Section 2

Security of personal data*Article 29***Security of processing**

1. Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

- (a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');
- (b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
- (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');
- (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
- (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');
- (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
- (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
- (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
- (i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

▼B

- (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

*Article 30***Notification of a personal data breach to the supervisory authority**

1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, 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.

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

3. The notification referred to in paragraph 1 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.

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

5. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, 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.

6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

▼B*Article 31***Communication of a personal data breach to the data subject**

1. Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
 - (a) the controller has implemented appropriate technological 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 a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.
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.
5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

Section 3**Data protection officer***Article 32***Designation of the data protection officer**

1. Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

▼B

2. The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34.

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

4. Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

*Article 33***Position of the data protection officer**

1. Member States shall provide for the controller to ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller shall support the data protection officer in performing the tasks referred to in Article 34 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.

*Article 34***Tasks of the data protection officer**

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

- (a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;
- (b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller 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 27;
- (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 28, and to consult, where appropriate, with regard to any other matter.

▼B*CHAPTER V**Transfers of personal data to third countries or international organisations**Article 35***General principles for transfers of personal data**

1. Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

- (a) the transfer is necessary for the purposes set out in Article 1(1);
- (b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);
- (c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;
- (d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and
- (e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.



Article 36

Transfers on the basis of an adequacy decision

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

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

- (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;
- (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 58(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3.

▼ B

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 58(3).

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

7. Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38.

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

*Article 37***Transfers subject to appropriate safeguards**

1. In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

- (a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or
- (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph 1.

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

▼B*Article 38***Derogations for specific situations**

1. In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

- (a) in order to protect the vital interests of the data subject or another person;
- (b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;
- (c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;
- (d) in individual cases for the purposes set out in Article 1(1); or
- (e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

*Article 39***Transfers of personal data to recipients established in third countries**

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

- (a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);
- (b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

▼B

- (c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;
- (d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;
- (e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

*Article 40***International cooperation for the protection of personal data**

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

- (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
- (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.



CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 41

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.
3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.
4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 42

Independence

1. Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.
2. Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.
3. Members of Member States' supervisory authorities shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

▼B

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

*Article 43***General conditions for the members of the supervisory authority**

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;
- their government;
- their head of State; or
- an independent body entrusted with the appointment under Member State law.

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

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

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

*Article 44***Rules on the establishment of the supervisory authority**

1. Each Member State shall provide by law for all of the following:

- (a) the establishment of each supervisory authority;
- (b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;
- (c) the rules and procedures for the appointment of the member or members of each supervisory authority;
- (d) the duration of the term of the member or members of each supervisory authority of not less than four years, except for the first appointment after 6 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
- (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
- (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

▼B

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

Section 2**Competence, tasks and powers***Article 45***Competence**

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

*Article 46***Tasks**

1. Each Member State shall provide, on its territory, for each supervisory authority to:

- (a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;
- (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;
- (c) advise, in accordance with Member State law, the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- (d) promote the awareness of controllers and processors of their obligations under this Directive;
- (e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

▼B

- (f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- (g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;
- (h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;
- (i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;
- (j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- (k) provide advice on the processing operations referred to in Article 28; and
- (l) contribute to the activities of the Board.

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

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

4. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

*Article 47***Powers**

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

▼B

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;
- (b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;
- (c) to impose a temporary or definitive limitation, including a ban, on processing.

3. Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

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

5. Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

*Article 48***Reporting of infringements**

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

*Article 49***Activity reports**

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of penalties imposed. Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, the Commission and the Board.



CHAPTER VII

Cooperation

Article 50

Mutual assistance

1. Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.
2. Each Member States shall provide for each supervisory authority to take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. The requested supervisory authority shall not refuse to comply with the request unless:
 - (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
 - (b) compliance with the request would infringe this Directive or Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
8. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

▼B*Article 51***Tasks of the Board**

1. The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in relation to processing within the scope of this Directive:

- (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;
- (b) 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 Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;
- (c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);
- (d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
- (e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);

▼C1

- (f) review the practical application of the guidelines, recommendations and best practices;

▼B

- (g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;
- (h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
- (i) 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;
- (j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

▼B

With regard to point (g) of the first subparagraph, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

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

3. The Board shall forward its opinions, guidelines, recommendations and best practices to the Commission and to the committee referred to in Article 58(1) and make them public.

4. The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

*CHAPTER VIII**Remedies, liability and penalties**Article 52***Right to lodge a complaint with a supervisory authority**

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.

3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

*Article 53***Right to an effective judicial remedy against a supervisory authority**

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

▼B

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.

3. Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

*Article 54***Right to an effective judicial remedy against a controller or processor**

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.

*Article 55***Representation of data subjects**

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.

*Article 56***Right to compensation**

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

*Article 57***Penalties**

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

▼B*CHAPTER IX****Implementing acts****Article 58***Committee procedure**

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

*CHAPTER X****Final provisions****Article 59***Repeal of Framework Decision 2008/977/JHA**

1. Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.
2. References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.

*Article 60***Union legal acts already in force**

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

*Article 61***Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation**

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

▼B*Article 62***Commission reports**

1. By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Directive to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.
3. For the purposes of paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.
6. By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

*Article 63***Transposition**

1. Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

▼B

3. By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

*Article 64***Entry into force**

This Directive shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

*Article 65***Addressees**

This Directive is addressed to the Member States.