



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 6 February 2013

6002/13

**Interinstitutional File:
2012/0010 (COD)**

**DATAPROTECT 9
JAI 73
DAPIX 11
FREMP 8
COMIX 55
CODEC 222**

NOTE

| | |
|-----------------|---|
| from: | General Secretariat |
| to: | Working Party on Information Exchange and Data Protection (DAPIX) |
| No. Cion prop.: | 5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 |
| Subject: | Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data |

Delegations find attached a comparative table prepared by the Commission Services in which the articles of the Commission proposal for a data protection Directive in criminal matters are put next to the proposal for a General Data Protection Regulation.

CHAPTER I

GENERAL PROVISIONS

| | | |
|--|--|--|
| <p>Article 1 Subject matter and objectives</p> <p>1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.</p> <p>2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.</p> <p>3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.</p> | <p>Article 1 Subject matter and objectives</p> <p>1. This Directive lays down the rules relating to the protection of individuals 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.</p> <p>In accordance with this Directive, Member States shall:</p> <p>(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and</p> <p>(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.</p> | |
| <p>Article 2 Material scope</p> <p>1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.</p> <p>2. This Regulation does not apply to the processing of personal data:</p> | <p>Article 2 Scope</p> <p>1. This Directive applies to the processing of personal data by competent authorities for the purposes referred to in Article 1(1).</p> <p>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.</p> <p>3. This Directive shall not apply to the processing of personal data:</p> | |

| | | |
|---|---|--|
| <p>(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;</p> | <p>(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;</p> | |
| <p>(b) by the Union institutions, bodies, offices and agencies;</p> | <p>(b) by the Union institutions, bodies, offices and agencies.</p> | |
| <p>(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;</p> | | |
| <p>(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;</p> | | |
| <p>(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.</p> | | |
| <p>3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.</p> | | |
| <p>Article 3 Territorial scope</p> | | |
| <p>1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.</p> | | |
| <p>2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:</p> | | |
| <p>(a) the offering of goods or services to such data subjects in the Union; or</p> | | |
| <p>(b) the monitoring of their behaviour.</p> | | |

| | | |
|--|---|--|
| <p>3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.</p> | | |
| <p>Article 4 Definitions</p> | <p>Article 3 Definitions</p> | |
| <p>For the purposes of this Regulation:</p> <p>(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p> <p>(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;</p> | <p>For the purposes of this Directive:</p> <p>(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p> <p>(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;</p> <p>(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;</p> | |
| | | |
| | | |

| | | |
|--|---|--|
| <p>(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;</p> | <p>(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;</p> | |
| <p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p> | <p>(6) 'controller' means the competent public authority which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p> | |
| <p>(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;</p> | <p>(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;</p> | |
| <p>(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;</p> | <p>(8) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;</p> | |
| <p>(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p> | | |
| <p>(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;</p> | <p>(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;</p> | |
| <p>(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;</p> | <p>(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;</p> | |
| <p>(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;</p> | <p>(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;</p> | |

| | | |
|---|---|--|
| <p>(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;</p> | <p>(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;</p> | |
| <p>(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;</p> | | |
| <p>(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;</p> | | |
| <p>(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;</p> | | |
| <p>(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;</p> | | |
| <p>(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;</p> | | |
| <p>(18) 'child' means any person below the age of 18 years;</p> | <p>(13) 'child' means any person below the age of 18 years;</p> | |

| | | |
|--|---|--|
| | <p>(14) 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;</p> | |
| | <p>(15) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.</p> | |
| <p>(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.</p> | | |

CHAPTER II PRINCIPLES

| Article 5 Principles relating to personal data processing | Article 4 Principles relating to personal data processing |
|---|--|
| Personal data must be: | Member States shall provide that personal data must be: |
| (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; | (a) processed fairly and lawfully; |
| (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; | (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; |
| (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; | (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed; |
| (d) accurate and 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; | (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 the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage; | (e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed; |

| | | |
|--|--|--|
| <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p> | <p>(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.</p> | |
| | <p>Article 5 Distinction between different categories of data subjects</p> | |
| | <p>1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:</p> | |
| | <p>(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;</p> | |
| | <p>(b) persons convicted of a criminal offence;</p> | |
| | <p>(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;</p> | |
| | <p>(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and</p> | |
| | <p>(e) persons who do not fall within any of the categories referred to above.</p> | |
| | <p>Article 6 Different degrees of accuracy and reliability of personal data</p> | |
| | <p>1. Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.</p> | |

| | | |
|--|---|--|
| | <p>2. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.</p> | |
| | <p>Article 7 Lawfulness of processing</p> | |
| | <p>Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary:</p> | |
| | | |
| | | |
| | (b) for compliance with a legal obligation to which the controller is subject; or | |
| | (c) in order to protect the vital interests of the data subject or of another person; or | |
| | (a) for the performance of a task carried out by a competent authority, based on law for the purposes set out in Article 1(1); or | |
| | (c) in order to protect the vital interests of the data subject or of another person; or | |
| | (d) for the prevention of an immediate and serious threat to public security. | |
| | | |
| | | |
| | | |

Article 6

Lawfulness of processing

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

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

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

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

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

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

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

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

| | | |
|--|--|--|
| <p>(b) the law of the Member State to which the controller is subject.</p> | | |
| <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> | | |
| <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> | | |
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p> | | |
| <p>Article 7</p> | | |
| <p>Conditions for consent</p> | | |
| <p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> | | |
| <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> | | |
| <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> | | |
| <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p> | | |

| | | |
|---|--|--|
| <p>Article 8 Processing of personal data of a child</p> <p>1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.</p> <p>2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> <p>4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| <p>Article 9 Processing of special categories of personal data</p> <p>1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.</p> | | |
| <p>Article 8 Processing of special categories of personal data</p> <p>1. Member States shall prohibit the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life.</p> | | |

| | | |
|---|--|--|
| <p>2. Paragraph 1 shall not apply where:</p> | <p>2. Paragraph 1 shall not apply where:</p> | |
| <p>(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or</p> <p>(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or</p> <p>(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or</p> <p>(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or</p> <p>(e) the processing relates to personal data which are manifestly made public by the data subject; or</p> | <p>(a) the processing is authorised by a law providing appropriate safeguards; or</p> | |
| <p>(b) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or</p> <p>(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or</p> <p>(e) the processing relates to personal data which are manifestly made public by the data subject; or</p> | <p>(b) the processing is necessary to protect the vital interests of the data subject or of another person; or</p> | |
| <p>(e) the processing relates to personal data which are manifestly made public by the data subject; or</p> | <p>(c) the processing relates to data which are manifestly made public by the data subject.</p> | |

| | | |
|---|--|--|
| <p>(f) processing is necessary for the establishment, exercise or defence of legal claims; or</p> <p>(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or</p> <p>(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or</p> <p>(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.</p> | | |
| <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.</p> | | |

| | | |
|---|--|--|
| Article 10 Processing not allowing identification | | |
| If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. | | |

CHAPTER III
RIGHTS OF THE DATA SUBJECT
[REGULATION] SECTION 1
TRANSPARENCY AND MODALITIES

| | | |
|---|--|--|
| <p>Article 11 Transparent information and communication</p> <p>1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.</p> <p>2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.</p> | <p>Article 10 Modalities for exercising the rights of the data subject</p> <p>1. Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.</p> <p>2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language.</p> | |
| <p>Article 12 Procedures and mechanisms for exercising the rights of the data subject</p> <p>1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.</p> | <p>Article 10 Modalities for exercising the rights of the data subject</p> <p>3. Member States shall provide that the controller takes all reasonable steps to establish procedures for providing the information referred to in Article 11 and for the exercise of the rights of data subjects referred to in Articles 12 to 17.</p> | |

| | | |
|--|---|--|
| <p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> | <p>4. Member States shall provide that the controller informs the data subject about the follow-up given to their request without undue delay.</p> | |
| <p>3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> | | |
| <p>4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.</p> | <p>5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are vexatious, in particular because of their repetitive character, or the size or volume of the request, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the vexatious character of the request.</p> | |

| | | |
|--|---|--|
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.</p> <p>6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| <p>Article 13 Rights in relation to recipients</p> <p>The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.</p> | | |
| | <p>Article 17 Rights of the data subject in criminal investigations and proceedings</p> <p>Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.</p> | |

**[REGULATION] SECTION 2
INFORMATION AND ACCESS TO DATA**

| <p>Article 14 Information to the data subject</p> | <p>Article 11 Information to the data subject</p> |
|--|--|
| <p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> | <p>1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller takes all appropriate measures to provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended;</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject;</p> <p>(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;</p> <p>(f) the recipients or categories of recipients of the personal data, including in third countries or international organisations;</p> |

| | |
|---|---|
| <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;</p> | |
| <p>(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p>3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.</p> | <p>(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> |
| <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are obtained from the data subject; or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> | |
| <p>5. Paragraphs 1 to 4 shall not apply, where:</p> | <p>3. The controller shall provide the information referred to in paragraph 1:</p> <p>(a) at the time when the personal data are obtained from the data subject, or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.</p> |
| <p>6. Paragraphs 1 to 4 shall not apply, where:</p> | <p>4. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject to the extent that, and as long as, such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned.</p> |

| | | |
|---|--|--|
| | (a) to avoid obstructing official or legal inquiries, investigations or procedures ; | |
| | (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; | |
| | (c) to protect public security; | |
| | (d) to protect national security; | |
| (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or | | |
| (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or | | |
| (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or | | |
| (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21. | (e) to protect the rights and freedoms of others. | |
| 6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests. | | |
| 7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises. | | |

| | | |
|---|--|--|
| <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| <p>Article 15 Right of access for the data subject</p> <p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> | <p>5. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 4.</p> | |
| <p>(a) the purposes of the processing;</p> | <p>(a) the purposes of the processing;</p> | |
| <p>(b) the categories of personal data concerned;</p> | <p>(b) the categories of personal data concerned;</p> | |
| <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> | <p>(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries;</p> | |
| <p>(d) the period for which the personal data will be stored;</p> | <p>(d) the period for which the personal data will be stored;</p> | |
| <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> | <p>(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;</p> | |
| <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> | <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> | |
| <p>(g) communication of the personal data undergoing processing and of any available information as to their source;</p> | <p>(g) communication of the personal data undergoing processing and of any available information as to their source.</p> | |

| | | |
|---|---|--|
| <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> | | |
| <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> | | |
| <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> | | |
| <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| | <p>2. <i>Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.</i></p> | |
| | <p>Article 13 Limitations to the right of access</p> | |
| | <p>1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned:</p> <p>(a) to avoid obstructing official or legal inquiries, investigations or procedures;</p> | |
| | | |

| | | |
|--|---|--|
| | (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties; | |
| | (c) to protect public security; | |
| | (d) to protect national security; | |
| | (e) to protect the rights and freedoms of others. | |
| | 2. Member States may determine by law categories of data processing which may wholly or partly fall under the exemptions of paragraph 1. | |
| | 3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject in writing on any refusal or restriction of access, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1. | |
| | 4. Member States shall ensure that the controller documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based. | |
| | Article 14 | |
| | Modalities for exercising the right of access | |
| | 1. Member States shall provide for the right of the data subject to request, in particular in cases referred to in Article 13, that the supervisory authority checks the lawfulness of the processing. | |
| | 2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1. | |
| | 3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question. | |

[REGULATION] SECTION 3 RECTIFICATION AND ERASURE

| | | |
|--|--|--|
| <p>Article 16 Right to rectification</p> <p>The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.</p> | <p>Article 15 Right to rectification</p> <p>1. Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, in particular by way of a corrective statement.</p> <p>2. Member States shall provide that the controller informs the data subject in writing on any refusal of rectification, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> | |
| <p>Article 17 Right to be forgotten and to erasure</p> <p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> | <p>Article 16 Right to erasure</p> <p>1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive.</p> | |

| | |
|--|--|
| <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> | |
| <p>2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> | |
| <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> | <p>2. The controller shall carry out the erasure without delay.</p> |
| <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> | |
| <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> | |
| <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> | |
| <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> | |
| <p>(e) in the cases referred to in paragraph 4.</p> | |
| <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> | <p>3. Instead of erasure, the controller shall mark the personal data where:</p> |
| <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> | <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> |
| <p>(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> | <p>(b) the personal data have to be maintained for purposes of proof;</p> |

| | | |
|---|---|--|
| (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; | (c) the data subject opposes their erasure and requests the restriction of their use instead. | |
| (d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2). | | |
| 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. | | |
| 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. | | |
| 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. | | |
| 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. | | |
| 9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: | | |
| (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; | | |
| (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; | | |
| (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4. | | |
| | 4. Member States shall provide that the controller informs the data subject in writing of any refusal of erasure or marking of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. | |

| | | |
|--|---|--|
| <p>Article 18 Right to data portability</p> <p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p> <p>2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p> <p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | <p>Article 12 Right of access for the data subject</p> <p>2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.</p> | |
| | | |
| | | |

**[REGULATION] SECTION 4
RIGHT TO OBJECT AND PROFILING**

| | | |
|---|---|--|
| <p>Article 19 Right to object</p> | | |
| <p>1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.</p> | | |
| <p>2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.</p> | | |
| <p>3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.</p> | | |
| <p>Article 20 Measures based on profiling</p> | | |
| <p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.</p> | <p>Article 9 Measures based on profiling and automated processing</p> <p>1. Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.</p> | |

| | | |
|---|---|--|
| <p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> | | |
| | | |
| | | |
| <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> | <p>2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.</p> | |
| <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> | | |
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p> | | |

**[REGULATION] SECTION 5
RESTRICTIONS**

| | | |
|---|--|--|
| <p>Article 21 Restrictions</p> <p>1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:</p> | | |
| (a) public security; | | |
| (b) the prevention, investigation, detection and prosecution of criminal offences; | | |
| (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity; | | |
| (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; | | |
| (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d); | | |
| (f) the protection of the data subject or the rights and freedoms of others. | | |
| 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller. | | |

**CHAPTER IV
CONTROLLER AND PROCESSOR
SECTION 1
GENERAL OBLIGATIONS**

| | | |
|--|---|--|
| <p>Article 22 Responsibility of the controller</p> <p>1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p>2. The measures provided for in paragraph 1 shall in particular include:</p> <p>(a) keeping the documentation pursuant to Article 28;</p> <p>(b) implementing the data security requirements laid down in Article 30;</p> <p>(c) performing a data protection impact assessment pursuant to Article 33;</p> <p>(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);</p> <p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> | <p>Article 18 Responsibility of the controller</p> <p>1. Member States shall provide that the controller adopts policies and implements appropriate measures to ensure that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.</p> <p>2. The measures referred to in paragraph 1 shall in particular include:</p> <p>(a) keeping the documentation referred to in Article 23;</p> <p>(c) implementing the data security requirements laid down in Article 27;</p> <p>(b) complying with the requirements for prior consultation pursuant to Article 26;</p> <p>(d) designating a data protection officer pursuant to Article 30.</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> | |
|--|---|--|

| | | |
|---|---|--|
| <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized enterprises.</p> | | |
| <p>Article 23 Data protection by design and by default</p> <p>1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> | <p>Article 19 Data protection by design and by default</p> <p>1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.</p> | |

| | |
|---|---|
| <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | |
| <p>Article 24 Joint controllers</p> <p>Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.</p> | <p>Article 20 Joint controllers</p> <p>Member States shall provide that where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.</p> |
| <p>Article 25 Representatives of controllers not established in the Union</p> | |
| <p>1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.</p> | |
| <p>2. This obligation shall not apply to:</p> | |
| <p>(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or</p> | |
| <p>(b) an enterprise employing fewer than 250 persons; or</p> | |
| <p>(c) a public authority or body; or</p> | |
| <p>(d) a controller offering only occasionally goods or services to data subjects residing in the Union.</p> | |
| <p>3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.</p> | |
| <p>4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.</p> | |

| | | |
|--|---|--|
| <p>Article 26 Processor</p> <p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> | <p>Article 21 Processor</p> <p>1. Member States shall provide that where a processing operation is carried out on behalf of a controller, the controller must choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.</p> <p>2. Member States shall provide that the carrying out of processing by a processor must be governed by a legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited.</p> | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|--|---|--|
| <p>(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;</p> | | |
| <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> | | |
| <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p> | | |
| <p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p> | <p>3. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 20.</p> | |
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</p> | | |
| <p>Article 27 Processing under the authority of the controller and processor</p> | <p>Article 22 Processing under the authority of the controller and processor</p> | |
| <p>The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.</p> | <p>Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.</p> | |
| <p>Article 28 Documentation</p> | <p>Article 23 Documentation</p> | |
| <p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> | <p>1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.</p> | |
| <p>2. The documentation shall contain at least the following information:</p> | <p>2. The documentation shall contain at least the following information:</p> | |

| | |
|---|--|
| (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; | (a) the name and contact details of the controller, or any joint controller or processor; |
| (b) the name and contact details of the data protection officer, if any; | |
| (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); | (b) the purposes of the processing; |
| (d) a description of categories of data subjects and of the categories of personal data relating to them; | |
| (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; | (c) the recipients or categories of recipients of the personal data; |
| (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; | (d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation. |
| (g) a general indication of the time limits for erasure of the different categories of data; | |
| (h) the description of the mechanisms referred to in Article 22(3). | |
| 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority. | 3. The controller and the processor shall make the documentation available, on request, to the supervisory authority. |
| 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: | |
| (a) a natural person processing personal data without a commercial interest; or | |
| (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. | |

| | | |
|--|---|--|
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> | | |
| <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| | <p>Article 24 Keeping of records</p> <p>1. Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data.</p> <p>2. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.</p> | |
| <p>Article 29 Co-operation with the supervisory authority</p> <p>1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.</p> | <p>Article 25 Cooperation with the supervisory authority</p> <p>1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing all information necessary for the supervisory authority to perform its duties.</p> | |

| | | |
|--|--|--|
| <p>2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.</p> | <p>2. In response to the supervisory authority's exercise of its powers under points (a) and (b) of Article 46, the controller and the processor shall reply to the supervisory authority within a reasonable period. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.</p> | |
|--|--|--|

SECTION 2 DATA SECURITY

| | | |
|--|--|--|
| <p>Article 30 Security of processing</p> <p>1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.</p> | <p>Article 27 Security of processing</p> <p>1. Member States shall provide that the controller and the processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.</p> <p>2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:</p> <p>(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);</p> <p>(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);</p> <p>(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);</p> <p>(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);</p> <p>(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);</p> <p>(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);</p> | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|--|---|--|
| | (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the 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 case of interruption, be restored (recovery); | |
| | (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). | |
| 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. | | |
| 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies. | | |

| | | |
|---|--|--|
| <p>4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <p>(a) prevent any unauthorised access to personal data;</p> <p>(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;</p> <p>(c) ensure the verification of the lawfulness of processing operations.</p> <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | <p>3. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).</p> | |
| <p>Article 31 Notification of a personal data breach to the supervisory authority</p> | <p>Article 28 Notification of a personal data breach to the supervisory authority</p> | |
| <p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> | <p>1. Member States shall provide that in the case of a personal data breach, the controller notifies, without undue delay and, where feasible, not later than 24 hours after having become aware of it, the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases where the notification is not made within 24 hours.</p> | |
| <p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> | <p>2. The processor shall alert and inform the controller immediately after having become aware of a personal data breach.</p> | |
| <p>3. The notification referred to in paragraph 1 must at least:</p> | <p>3. The notification referred to in paragraph 1 shall at least:</p> | |
| <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> | <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> | |
| <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p> | <p>(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;</p> | |

| | | |
|---|---|--|
| (c) recommend measures to mitigate the possible adverse effects of the personal data breach; | (c) recommend measures to mitigate the possible adverse effects of the personal data breach; | |
| (d) describe the consequences of the personal data breach; | (d) describe the possible consequences of the personal data breach; | |
| (e) describe the measures proposed or taken by the controller to address the personal data breach. | (e) describe the measures proposed or taken by the controller to address the personal data breach. | |
| 4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. | 4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. | |
| 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach. | 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach. | |
| 6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). | 6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2). | |
| Article 32 Communication of a personal data breach to the data subject | Article 29 Communication of a personal data breach to the data subject | |
| 1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. | 1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay. | |

| | | |
|--|--|--|
| <p>2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).</p> <p>3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> | <p>2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 28(3).</p> <p>3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.</p> | |
| <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| | <p>4. The communication to the data subject may be delayed, restricted or omitted on the grounds referred to in Article 11(4).</p> | |

**[REGULATION] SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION**

| | | |
|---|--|--|
| <p>Article 33 Data protection impact assessment</p> | | |
| <p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> | | |
| <p>2. The following processing operations in particular are likely to present specific risks referred to in paragraph 1:</p> | | |
| <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> | | |
| <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> | | |
| <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> | | |
| <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> | | |
| <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> | | |

| | | |
|---|--|--|
| <p>3. The assessment 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 the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> | | |
| <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> | | |
| <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p> | | |
| <p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> | | |
| <p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |

| | | |
|---|--|--|
| <p>Article 34 Prior authorisation and prior consultation</p> <p>1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p> <p>(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or</p> <p>(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.</p> <p>3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.</p> | <p>Article 26 Prior consultation of the supervisory authority</p> <p>1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new filing system to be created where:</p> <p>(a) special categories of data referred to in Article 8 are to be processed;</p> <p>(b) the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.</p> <p>2. Member States may provide that the supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.</p> | |
|---|--|--|

| | | |
|--|--|--|
| <p>4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.</p> | | |
| <p>5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.</p> | | |
| <p>6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 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.</p> | | |
| <p>7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.</p> | | |
| <p>8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.</p> | | |
| <p>9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |

**[REGULATION] SECTION 4 / [DIRECTIVE] SECTION 3
DATA PROTECTION OFFICER**

| | | |
|--|---|--|
| <p>Article 35 Designation of the data protection officer</p> <p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> | <p>Article 30 Designation of the data protection officer</p> <p>1. Member States shall provide that the controller or the processor designates a data protection officer.</p> | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | <p>3. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.</p> | |
| | | |
| | | |
| | <p>2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.</p> | |

| | | |
|---|--|--|
| <p>6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> | | |
| <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> | | |
| <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> | | |
| <p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.</p> | | |
| <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> | | |
| <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p> | | |
| <p>Article 36 Position of the data protection officer</p> | | |
| <p>1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.</p> | <p>Article 31 Position of the data protection officer</p> <p>1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.</p> | |

| | | | | | | |
|--|---|--|--|--|--|--|
| <p>2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> | <p>2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.</p> | | | | | |
| <p>3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p> | | | | | | |
| <p>Article 37 Tasks of the data protection officer</p> | | | <p>Article 32 Tasks of the data protection officer</p> | | | |
| <p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> | <p>Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:</p> | | | | | |
| <p>(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> | <p>(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive and to document this activity and the responses received;</p> | | | | | |
| <p>(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> | <p>(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;</p> | | | | | |
| <p>(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p> | <p>(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;</p> | | | | | |
| <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> | <p>(d) to ensure that the documentation referred to in Article 23 is maintained;</p> | | | | | |
| <p>(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;</p> | <p>(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;</p> | | | | | |

| | | |
|---|--|--|
| <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;</p> | <p>(f) to monitor the application for prior consultation to the supervisory authority, if required pursuant to Article 26 ;</p> | |
| <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> | <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;</p> | |
| <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> | <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.</p> | |
| <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.</p> | | |

**[REGULATION] SECTION 5
CODES OF CONDUCT AND CERTIFICATION**

| | |
|--|--|
| <p>Article 38 Codes of conduct</p> | |
| <p>1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:</p> | |
| <p>(a) fair and transparent data processing;</p> | |
| <p>(b) the collection of data;</p> | |
| <p>(c) the information of the public and of data subjects;</p> | |
| <p>(d) requests of data subjects in exercise of their rights;</p> | |
| <p>(e) information and protection of children;</p> | |
| <p>(f) transfer of data to third countries or international organisations;</p> | |
| <p>(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;</p> | |
| <p>(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.</p> | |
| <p>2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.</p> | |

| | | |
|---|--|--|
| <p>3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.</p> | | |
| <p>4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p> | | |
| <p>5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.</p> | | |
| <p>Article 39 Certification</p> | | |
| <p>1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.</p> | | |
| <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.</p> | | |

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

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

| | | |
|---|--|--|
| <p>Article 40 General principle for transfers</p> <p>Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.</p> | <p>Article 33 General principles for transfers of personal data</p> <p>Member States shall provide that any transfer of personal data by competent authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:</p> <p>(a) the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and</p> <p>(b) the conditions laid down in this Chapter are complied with by the controller and processor.</p> | |
| <p>Article 41 Transfers with an adequacy decision</p> <p>1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.</p> <p>2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:</p> | <p>Article 34 Transfers with an adequacy decision</p> <p>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 in accordance with Article 41 of Regulation (EU) .../2012 or in accordance with paragraph 3 of this Article that the third country or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.</p> <p>2. Where no decision adopted in accordance with Article 41 of Regulation (EU) .../2012 exists, the Commission shall assess the adequacy of the level of protection, giving consideration to the following elements:</p> | |

| | | |
|--|---|--|
| <p>(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;</p> | <p>(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law as well as the security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;</p> | <p>(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;</p> |
| <p>(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and</p> | <p>(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subject in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and</p> | <p>(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and</p> |
| <p>(c) the international commitments the third country or international organisation in question has entered into.</p> | <p>(c) the international commitments the third country or international organisation in question has entered into.</p> | <p>(c) the international commitments the third country or international organisation in question has entered into.</p> |
| <p>3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with Article 87(2).</p> | <p>3. The Commission may decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).</p> | <p>3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> |
| <p>4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.</p> | <p>4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.</p> | <p>4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.</p> |

| | | |
|---|--|--|
| <p>5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including administrative and judicial redress for data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency with respect to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> | <p>5. The Commission may decide within the scope of this Directive that a third country or a territory or a processing sector within that third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 57(3).</p> | <p>5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency with respect to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> |
| <p>6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.</p> | <p>6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.</p> | <p>6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.</p> |
| <p>7. The Commission shall publish in the <i>Official Journal of the European Union</i> a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.</p> | <p>7. The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.</p> | <p>7. The Commission shall publish in the <i>Official Journal of the European Union</i> a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.</p> |

| | | |
|---|---|--|
| <p>8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.</p> | | |
| <p>Article 42 Transfers by way of appropriate safeguards</p> <p>1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p> | <p>Article 35 Transfers by way of appropriate safeguards</p> <p>1. Where the Commission has taken no decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a recipient in a third country or an international organisation may take place where:</p> <p>(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or</p> <p>(b) the controller or processor has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.</p> <p>2. The decision for transfers under paragraph 1 (b) must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request.</p> | |
| <p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or</p> | | |

| | | |
|--|--|--|
| <p>(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.</p> | | |
| <p>3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.</p> | | |
| <p>4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p> | | |
| <p>5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.</p> | | |

| | | | | | | | | | | | | | | | | | | | | | |
|---|--|---|--|---|--|--|--|--|--|---|--|--|--|---|--|--|--|---|--|---|--|
| <p>Article 43 Transfers by way of binding corporate rules</p> | | <p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> | | <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;</p> | | <p>(b) expressly confer enforceable rights on data subjects;</p> | | <p>(c) fulfil the requirements laid down in paragraph 2.</p> | | <p>2. The binding corporate rules shall at least specify:</p> | | <p>(a) the structure and contact details of the group of undertakings and its members;</p> | | <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> | | <p>(c) their legally binding nature, both internally and externally;</p> | | <p>(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;</p> | | <p>(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> | |
|---|--|---|--|---|--|--|--|--|--|---|--|--|--|---|--|--|--|---|--|---|--|

| | | |
|--|--|--|
| <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;</p> | | |
| <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;</p> | | |
| <p>(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;</p> | | |
| <p>(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;</p> | | |
| <p>(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;</p> | | |
| <p>(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.</p> | | |
| <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> | | |

| | | |
|--|---|--|
| <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p> | | |
| <p>Article 44 Derogations</p> | <p>Article 36 Derogations</p> | |
| <p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> | <p>By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:</p> | |
| <p>(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or</p> | | |
| <p>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or</p> | | |
| <p>(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or</p> | | |
| <p>(d) the transfer is necessary for important grounds of public interest; or</p> | <p>(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or</p> <p>(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or</p> | |
| <p>(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or</p> | <p>(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.</p> | |

| | | |
|---|---|--|
| <p>(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or</p> | <p>(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or (b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or</p> | |
| <p>(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or</p> | | |
| <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> | | |
| <p>2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.</p> | | |
| <p>3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> | | |

| | | |
|---|---|--|
| <p>4. Points (a), (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.</p> | | |
| <p>5. The public interest referred to in point d of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p> | | |
| <p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p> | | |
| <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.</p> | | |
| | <p>Article 37 Specific conditions for the transfer of personal data</p> | |
| | <p>Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met.</p> | |
| <p>Article 45 International co-operation for the protection of personal data</p> | <p>Article 38 International co-operation for the protection of personal data</p> | |
| <p>1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:</p> | <p>1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:</p> | |
| <p>(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;</p> | <p>(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;</p> | |
| <p>(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;</p> | <p>(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;</p> | |

| | | |
|---|--|--|
| <p>(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;</p> | <p>(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;</p> | |
| <p>(d) promote the exchange and documentation of personal data protection legislation and practice.</p> | <p>(d) promote the exchange and documentation of personal data protection legislation and practice.</p> | |
| <p>2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).</p> | <p>2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).</p> | |

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES
SECTION 1
INDEPENDENT STATUS

| | | |
|---|---|--|
| <p>Article 46 Supervisory authority</p> <p>1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.</p> | <p>Article 39 Supervisory authority</p> <p>1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.</p> | |
| | <p>2. Member States may provide that the supervisory authority established in Member States pursuant to Regulation (EU).../2012 assumes responsibility for the tasks of the supervisory authority to be established pursuant to paragraph 1 of this Article.</p> | |
| <p>2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.</p> | <p>3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.</p> | |

| | | |
|--|--|--|
| <p>3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p> | | |
| <p>Article 47 Independence</p> | <p>Article 40 Independence</p> | |
| <p>1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.</p> | <p>1. Member States shall ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it.</p> | |
| <p>2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.</p> | <p>2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody.</p> | |
| <p>3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.</p> | <p>3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.</p> | |
| <p>4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.</p> | <p>4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.</p> | |
| <p>5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.</p> | <p>5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.</p> | |
| <p>6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.</p> | <p>6. Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.</p> | |
| <p>7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.</p> | <p>7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.</p> | |

| | |
|---|--|
| <p>Article 48 General conditions for the members of the supervisory authority</p> <p>1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.</p> <p>2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.</p> <p>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 paragraph 5.</p> <p>4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.</p> <p>5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.</p> <p>Article 49 Rules on the establishment of the supervisory authority</p> <p>Each Member State shall provide by law within the limits of this Regulation:</p> <p>(a) the establishment and status of the supervisory authority;</p> <p>(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;</p> <p>(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;</p> | <p>Article 41 General conditions for the members of the supervisory authority</p> <p>1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.</p> <p>2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.</p> <p>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 paragraph 5.</p> <p>4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.</p> <p>5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.</p> <p>Article 42 Rules on the establishment of the supervisory authority</p> |
|---|--|

| | | |
|---|--|--|
| <p>(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;</p> | | |
| <p>(e) whether the members of the supervisory authority shall be eligible for reappointment;</p> | | |
| <p>(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;</p> | | |
| <p>(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.</p> | | |
| <p>Article 50 Professional secrecy</p> | <p>Article 43 Professional secrecy</p> | |
| <p>The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.</p> | <p>Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.</p> | |

SECTION 2 DUTIES AND POWERS

| | | |
|--|---|--|
| <p>Article 51 Competence</p> <p>1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.</p> <p>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p> | <p>Article 44 Competence</p> <p>1. Member States shall provide that each supervisory authority exercises, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.</p> | |
| <p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p> | <p>2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity.</p> | |
| <p>Article 52 Duties</p> <p>1. The supervisory authority shall:</p> <p>(a) monitor and ensure the application of this Regulation;</p> | <p>Article 45 Duties</p> <p>1. Member States shall provide that the supervisory authority:</p> <p>(a) monitors and ensures the application of the provisions adopted pursuant to this Directive and its implementing measures;</p> | |

| | | |
|--|--|--|
| <p>(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;</p> | <p>(b) hears complaints lodged by any data subject, or by an association representing and duly mandated by that data subject in accordance with Article 50, investigates, to the extent appropriate, the matter and informs the data subject the association of the progress and the outcome of the complaint within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;</p> | |
| | <p>(c) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;</p> | |
| <p>(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;</p> | <p>(d) provides mutual assistance to other supervisory authorities and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;</p> | |
| <p>(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;</p> | <p>(e) conducts investigations either on its own initiative or on the basis of a complaint, or on request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;</p> | |
| <p>(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;</p> | <p>(f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;</p> | |
| <p>(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;</p> | <p>(g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;</p> | |
| <p>(g) authorise and be consulted on the processing operations referred to in Article 34;</p> | <p>(h) is consulted on processing operations pursuant to Article 26;</p> | |
| <p>(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);</p> | | |
| <p>(i) approve binding corporate rules pursuant to Article 43;</p> | | |
| <p>(j) participate in the activities of the European Data Protection Board.</p> | <p>(i) participates in the activities of the European Data Protection Board.</p> | |

| | | |
|--|--|--|
| <p>2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.</p> | <p>2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.</p> | |
| <p>3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.</p> | <p>3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.</p> | |
| <p>4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.</p> | <p>4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.</p> | |
| <p>5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.</p> | <p>5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.</p> | |
| <p>6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.</p> | <p>6. Where requests are vexatious, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action required by the data subject. The supervisory authority shall bear the burden of proving of the vexatious character of the request.</p> | |

| | |
|---|--|
| <p>Article 53 Powers</p> | |
| <p>1. Each supervisory authority shall have the power:</p> | |
| <p>(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;</p> | |
| <p>(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;</p> | |
| <p>(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;</p> | |
| <p>(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;</p> | |
| <p>(e) to warn or admonish the controller or the processor;</p> | |
| <p>(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;</p> | |
| <p>(g) to impose a temporary or definitive ban on processing;</p> | |
| <p>(h) to suspend data flows to a recipient in a third country or to an international organisation;</p> | |
| <p>(i) to issue opinions on any issue related to the protection of personal data;</p> | |
| <p>(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.</p> | |
| <p>Article 46 Powers</p> | |
| <p>Member States shall provide that each supervisory authority must in particular be endowed with:</p> | |
| <p>(b) effective powers of intervention, such as the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller, or referring the matter to national parliaments or other political institutions ;</p> | |

| | | |
|--|--|--|
| <p>2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:</p> | <p>(a) investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;</p> | |
| <p>(a) access to all personal data and to all information necessary for the performance of its duties;</p> | | |
| <p>(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.</p> | | |
| <p>The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.</p> | | |
| <p>3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).</p> | <p>(c) the power to engage in legal proceedings where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of the judicial authorities.</p> | |
| <p>4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).</p> | | |
| <p>Article 54 Activity report</p> | <p>Article 47 Activities report</p> | |
| <p>Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.</p> | <p>Member States shall provide that each supervisory authority draws up an annual report on its activities. The report shall be made available to the Commission and the European Data Protection Board.</p> | |

CHAPTER VII
[Regulation] CO-OPERATION and Consistency / [Directive] CO-OPERATION
[REGULATION] SECTION 1
CO-OPERATION

| | | |
|---|--|--|
| <p>Article 55 Mutual assistance</p> <p>1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.</p> | <p>Article 48 Mutual assistance</p> <p>1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.</p> | |
| <p>2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.</p> | <p>2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority.</p> | |
| <p>3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.</p> | | |

| | | |
|--|--|--|
| <p>4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:</p> <p>(a) it is not competent for the request; or</p> <p>(b) compliance with the request would be incompatible with the provisions of this Regulation.</p> | | |
| <p>5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.</p> | <p>3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.</p> | |
| <p>6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.</p> | | |
| <p>7. No fee shall be charged for any action taken following a request for mutual assistance.</p> | | |
| <p>8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.</p> | | |
| <p>9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> | | |

| | | | |
|---|--|--|--|
| <p>10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | | |
| <p>Article 56 Joint operations of supervisory authorities</p> <p>1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.</p> <p>2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay.</p> | | | |

| | | |
|--|--|--|
| <p>3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.</p> | | |
| <p>4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.</p> | | |
| <p>5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).</p> | | |
| <p>6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.</p> | | |

**[REGULATION] SECTION 2
CONSISTENCY**

| | | |
|---|--|--|
| <p>Article 57 Consistency mechanism For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.</p> | | |
| <p>Article 58 Opinion by the European Data Protection Board 1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> | | |
| <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p> | | |
| <p>(b) may substantially affect the free movement of personal data within the Union; or</p> | | |
| <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> | | |
| <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> | | |
| <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> | | |
| <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> | | |

| | | |
|--|--|--|
| <p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operation in accordance with Article 56.</p> | | |
| <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.</p> | | |
| <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p> | | |
| <p>6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.</p> | | |
| <p>7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.</p> | | |

| | | |
|---|--|--|
| <p>8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.</p> | | |
| <p>Article 59 Opinion by the Commission</p> | | |
| <p>1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.</p> | | |
| <p>2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.</p> | | |
| <p>3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.</p> | | |
| <p>4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.</p> | | |

| | | | |
|---|--|--|--|
| <p>Article 60 Suspension of a draft measure</p> | <p>1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:</p> <p>(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or</p> <p>(b) adopt a measure pursuant to point (a) of Article 62(1).</p> <p>2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.</p> <p>3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.</p> | | |
| <p>Article 61 Urgency procedure</p> | <p>1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> | | |

| | | |
|---|--|--|
| <p>2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.</p> | | |
| <p>3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.</p> | | |
| <p>4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.</p> | | |
| <p>Article 62 Implementing acts</p> | | |
| <p>1. The Commission may adopt implementing acts for:</p> | | |
| <p>(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;</p> | | |
| <p>(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;</p> | | |
| <p>(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;</p> | | |

| | | |
|--|--|--|
| <p>(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).</p> | | |
| <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> | | |
| <p>2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.</p> | | |
| <p>3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.</p> | | |
| <p>Article 63 Enforcement</p> | | |
| <p>1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.</p> | | |
| <p>2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.</p> | | |

**[REGULATION] SECTION 3
EUROPEAN DATA PROTECTION BOARD**

| | |
|--|--|
| <p>Article 64 European Data Protection Board</p> | |
| <p>1. A European Data Protection Board is hereby set up.</p> | |
| <p>2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.</p> | |
| <p>3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.</p> | |
| <p>4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.</p> | |
| <p>Article 65 Independence</p> | |
| <p>1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.</p> | |
| <p>2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.</p> | |

| | | |
|--|--|--|
| <p>Article 66 Tasks of the European Data Protection Board</p> <p>1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:</p> | <p>Article 49 Tasks of the European Data Protection Board</p> <p>1. The European Data Protection Board established by Regulation (EU) .../2012 shall exercise the following tasks in relation to processing within the scope of this Directive:</p> | |
| <p>(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> | <p>(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;</p> | |
| <p>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;</p> | <p>(b) examine, on request of the Commission or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of those provisions;</p> | |
| <p>(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> | <p>(c) review the practical application of guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> | |
| <p>(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;</p> | <p>(d) give the Commission an opinion on the level of protection in third countries or international organisations;</p> | |
| <p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> | <p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> | |
| <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> | <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> | |
| <p>(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.</p> | <p>(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice.</p> | |

| | | |
|---|---|--|
| <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> | <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> | |
| <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.</p> | <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.</p> | |
| <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p> | <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p> | |
| <p>Article 67 Reports</p> | | |
| <p>1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries. The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).</p> | | |
| <p>2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.</p> | | |
| <p>Article 68 Procedure</p> | | |
| <p>1. The European Data Protection Board shall take decisions by a simple majority of its members.</p> | | |
| <p>2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.</p> | | |

| | | |
|---|--|--|
| Article 69 Chair | | |
| 1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair. | | |
| 2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable. | | |
| Article 70 Tasks of the chair | | |
| 1. The chair shall have the following tasks: | | |
| (a) to convene the meetings of the European Data Protection Board and prepare its agenda; | | |
| (b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57. | | |
| 2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure. | | |
| Article 71 Secretariat | | |
| 1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat. | | |
| 2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair. | | |
| 3. The secretariat shall be responsible in particular for: | | |
| (a) the day-to-day business of the European Data Protection Board; | | |
| (b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public; | | |
| (c) the use of electronic means for the internal and external communication; | | |

| | | |
|---|--|--|
| (d) the translation of relevant information; | | |
| (e) the preparation and follow-up of the meetings of the European Data Protection Board; | | |
| (f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board. | | |
| Article 72 | | |
| Confidentiality | | |
| 1. The discussions of the European Data Protection Board shall be confidential. | | |
| 2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation No 1049/2001 or the European Data Protection Board otherwise makes them public. | | |
| 3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them. | | |

CHAPTER VIII REMEDIES, LIABILITY AND SANCTIONS

| | | |
|---|---|--|
| <p>Article 73 Right to lodge a complaint with a supervisory authority</p> <p>1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.</p> <p>2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.</p> <p>3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.</p> | <p>Article 50 Right to lodge a complaint with a supervisory authority</p> <p>1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.</p> <p>2. Member States shall provide for the right of any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and is being properly constituted according to the law of a Member State to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data. The organisation or association must be duly mandated by the data subject(s).</p> <p>3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.</p> | |
|---|---|--|

| | |
|---|--|
| <p>Article 74 Right to a judicial remedy against a supervisory authority</p> <p>1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.</p> <p>2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).</p> <p>3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.</p> <p>4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.</p> <p>5. The Member States shall enforce final decisions by the courts referred to in this Article.</p> | <p>Article 51 Right to a judicial remedy against a supervisory authority</p> <p>1. Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.</p> <p>2. Each data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).</p> <p>3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.</p> |
| <p>Article 75 Right to a judicial remedy against a controller or processor</p> <p>1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.</p> | <p>Article 52 Right to a judicial remedy against a controller or processor</p> <p>Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.</p> |

| | | |
|---|--|--|
| <p>2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.</p> | | |
| <p>3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.</p> | | |
| <p>4. The Member States shall enforce final decisions by the courts referred to in this Article.</p> | | |
| <p>Article 76 Common rules for court proceedings</p> | <p>Article 53 Common rules for court proceedings</p> | |
| <p>1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.</p> | <p>1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51 and 52 on behalf of one or more data subjects.</p> | |
| <p>2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.</p> | <p>2. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.</p> | |
| <p>3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.</p> | | |
| <p>4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.</p> | | |

| | |
|--|--|
| <p>5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.</p> | <p>3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.</p> |
| <p>Article 77 Right to compensation and liability</p> | <p>Article 54 Liability and the right to compensation</p> |
| <p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.</p> | <p>1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that they are not responsible for the event giving rise to the damage.</p> |
| <p>Article 78 Penalties</p> | <p>Article 55 Penalties</p> |
| <p>1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.</p> <p>2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.</p> <p>3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p> | <p>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 must be effective, proportionate and dissuasive.</p> |

| | | |
|---|--|--|
| <p>Article 79 Administrative sanctions</p> | | |
| <p>1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.</p> | | |
| <p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.</p> | | |
| <p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> | | |
| <p>(a) a natural person is processing personal data without a commercial interest; or</p> | | |
| <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> | | |
| <p>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> | | |
| <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> | | |
| <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> | | |

| | | |
|---|--|--|
| <p>5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> | | |
| <p>(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;</p> | | |
| <p>(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;</p> | | |
| <p>(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;</p> | | |
| <p>(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;</p> | | |
| <p>(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;</p> | | |
| <p>(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);</p> | | |
| <p>(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.</p> | | |

| | | | |
|---|--|--|--|
| 6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: | | | |
| (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; | | | |
| (b) processes special categories of data in violation of Articles 9 and 81; | | | |
| (c) does not comply with an objection or the requirement pursuant to Article 19; | | | |
| (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; | | | |
| (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; | | | |
| (f) does not designate a representative pursuant to Article 25; | | | |
| (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27; | | | |
| (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32; | | | |
| (i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34; | | | |
| (j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37; | | | |
| (k) misuses a data protection seal or mark in the meaning of Article 39; | | | |
| (l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44; | | | |

| | | |
|--|--|--|
| <p>(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);</p> | | |
| <p>(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);</p> | | |
| <p>(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.</p> | | |
| <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p> | | |

[Regulation] CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

| | |
|---|--|
| <p>Article 80 Processing of personal data and freedom of expression</p> | |
| <p>1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.</p> | |
| <p>2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.</p> | |
| <p>Article 81 Processing of personal data concerning health</p> | |
| <p>1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:</p> | |

| | | |
|---|--|--|
| <p>(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or</p> | | |
| <p>(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or</p> | | |
| <p>(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.</p> | | |
| <p>2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.</p> | | |
| <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.</p> | | |

| | | |
|---|--|--|
| <p>Article 82 Processing in the employment context</p> <p>1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.</p> <p>2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1...</p> | | |
| <p>Article 83 Processing for historical, statistical and scientific research purposes</p> <p>1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:</p> <p>(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;</p> <p>(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.</p> | | |

| | | |
|---|--|--|
| <p>2. Bodies conducting historical, statistical or scientific research may publish personal data only if:</p> | | |
| <p>(a) the data subject has given consent, subject to the conditions laid down in Article 7;</p> | | |
| <p>(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or</p> | | |
| <p>(c) the data subject has made the data public.</p> | | |
| <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.</p> | | |
| <p>Article 84 Obligations of secrecy</p> | | |
| <p>1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.</p> | | |
| <p>2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p> | | |

| | | |
|---|--|--|
| <p>Article 85 Existing data protection rules of churches and religious associations</p> <p>1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.</p> <p>2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.</p> | | |
|---|--|--|

[Regulation] CHAPTER X / [Directive] CHAPTER IX DELEGATED ACTS AND IMPLEMENTING ACTS

| <p>Article 86 Exercise of the delegation</p> | <p>Article 56 Exercise of the delegation</p> | |
|--|---|--|
| <p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p> <p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> | <p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 28(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.</p> <p>3. The delegation of power referred to in Article 28(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> | |
| | | |

| | | |
|---|---|--|
| <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> | <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> | |
| <p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p> | <p>5. A delegated act adopted pursuant to Article 28(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or the Council.</p> | |
| <p>Article 87 Committee procedure</p> | <p>Article 57 Committee procedure</p> | |
| <p>1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p> | <p>1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p> | |
| <p>2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p> | <p>2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p> | |
| <p>3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.</p> | <p>3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.</p> | |

**[Regulation] CHAPTER XI / [Directive] CHAPTER X
FINAL PROVISIONS**

| | |
|--|--|
| <p>Article 88 Repeal of Directive 95/46/EC</p> | <p>Article 58 Repeals</p> |
| <p>1. Directive 95/46/EC is repealed.</p> <p>2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.</p> | <p>1. Council Framework Decision 2008/977/JHA is repealed.</p> <p>2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.</p> |
| <p>Article 89 Relationship to and amendment of Directive 2002/58/EC</p> | <p>Article 59 Relation with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation</p> |
| <p>1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.</p> <p>2. Article 1(2) of Directive 2002/58/EC shall be deleted.</p> | <p>The specific provisions for the protection of personal data with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data 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 remain unaffected.</p> |

| | | |
|---|---|--|
| | <p>Article 60 Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation</p> <p>International agreements concluded by Member States prior to the entry into force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.</p> | |
| <p>Article 90 Evaluation</p> | <p>Article 61 Evaluation</p> <p>1. The Commission shall evaluate the application of this Directive.</p> <p>2. The Commission shall review within three years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.</p> | |
| <p>The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.</p> | <p>3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.</p> | |

| | |
|---|--|
| | |
| | <p>Article 62 Implementation</p> <p>1. Member States shall adopt and publish, by [date/ two years after entry into force] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.</p> <p>They shall apply those provisions from xx.xx.201x [date/ two years after entry into force].</p> <p>When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.</p> <p>2. 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.</p> |
| <p>Article 91 Entry into force and application</p> <p>1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>2. It shall apply from [two years from the date referred to in paragraph 1].</p> <p>This Regulation shall be binding in its entirety and directly applicable in all Member States.</p> | |
| | |
| | <p>Article 63 Entry into force and application</p> <p>This Directive shall enter into force on the first day following that of its publication in the Official Journal of the European Union.</p> |
| | |
| | <p>Article 64 Addressees</p> <p>This Directive is addressed to the Member States.</p> |
