COUNCIL OF THE EUROPEAN UNION

Brussels, 28 June 2013

11624/13

Interinstitutional File: 2012/0010 (COD)

LIMITE

DATAPROTECT 83
JAI 570
DAPIX 90
FREMP 96
COMIX 403
CODEC 1618

NOTE

from:	Presidency
to:	delegations
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 revised text of the above Directive drawn up by the Presidency on the basis of delegations' comments and taking into account comments made on the draft general Data Protection Regulation that are relevant for this Directive.[1]

All changes made to the original Commission proposal are underlined text, or, where text has been deleted, indicated by (…). Where text has been moved, this text is indicated in italics.

_____

[1] A further version of this draft of the Directive containing Member State comments set out in footnotes will be distributed in due course.

ANNEX

2012/0010 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

After consulting the European Data Protection Supervisor[1],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.

[1] OJ C… , p. .

(2) The (…) principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

(4) This requires facilitating the free flow of data between competent public authorities within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[2] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

---

1 OJ L 281, 23.11.1995, p. 31.
2 OJ L 350, 30.12.2008, p. 60.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent public authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintenance of public order,] or the execution of criminal penalties should be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation EU …../2012 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintainance of public order,] or the execution of criminal penalties.

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent public authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of judicial co-operation in criminal matters and police co-operation. The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union.

(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.

(15) The protection of individuals should be technologically neutral and not depend on the technologies, mechanisms or procedures used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, such as an activity concerning national security, taking into account Articles 3 and 6 of the Treaty on the Functioning of the European Union, nor to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.

(15a) Regulation (EC) No 45/2001[1] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation EU …../2012.

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable.

(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.

(17) Personal data relating to health should include in particular (…) data pertaining to the health status of a data subject, (…) including any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(18) Any processing of personal data must be (…) lawful in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit.

[1] OJ L 8, 12.1.2001, p. 1.

(19) For the prevention, investigation and prosecution of criminal offences [and for these purposes, the maintenance of public order], it is necessary for competent public authorities to retain and process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

(20) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. In general, further processing for historical, statistical or scientific purposes should not be considered as incompatible with the original purpose of processing. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. (…). Personal data which are inaccurate should be rectified or erased.

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(22) In the interpretation and application of the general principles relating to personal data processing by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintenance of public order,] or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued.

(23) It is characteristic to the processing of personal data (…) by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintenance of public order,] or the execution of criminal penalties that personal data relating to different categories of data subjects are processed. Therefore, the competent public authorities (…) should, as far as possible, make a distinction between personal data of different categories of data subjects such as persons convicted of a criminal offence, suspects, (…) victims and third parties. (…).

(24) Furthermore, (…) personal data should be distinguished, as far as possible, according to the degree of their accuracy and reliability; (…) facts should be distinguished from personal assessments in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent public authorities.

(25) In order to be lawful, the processing of personal data should be necessary for (…) the performance of a task carried out in the public interest by a competent public authority based on Union law or Member State law or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate and serious threat to public security.

(25a) Member States should provide that where Union law or the national law applicable to the transmitting competent public authority provides for specific conditions applicable in specific circumstances to the processing of personal data, the transmitting public authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. These obligations apply also to transfers to recipients in third countries or international organisations. Member States should provide that the transmitting public authority does not apply conditions pursuant to paragraph 1 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to the transmitting public authority.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights (…) and freedoms, including genetic data, deserve specific protection. This should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is specifically authorised by a law which provides for (…) appropriate safeguards for the rights and freedoms of the data subjects; or the processing is necessary to protect the vital interests of the data subject or of another person; or the processing is necessary for the prevention of an immediate and serious threat to public security (…).

(27) Every data subject should have the right not to be subject to a decision which is based solely on profiling (…), unless authorised by law and subject to appropriate safeguards for the rights and freedoms of the data subject (…).

(28) In order to exercise their rights, any information to the data subject should be easily accessible and easy to understand, requiring the use of clear and plain language.

(29) Modalities should be provided for facilitating the data subject's exercise of their rights under the provisions adopted pursuant to this Directive, including mechanisms to request, free of charge, (…) access to data, as well as rectification, erasure and restriction. The controller should be obliged to respond to requests of the data subject without undue delay.

(30) (…) The data subjects should be informed of at least (…) the identity of the controller, the existence of the processing operation and its purposes, (…) and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, if they do not provide such data.

(31) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not obtained from the data subject (…), within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed or if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

(32) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, where possible for what period, and which recipients receive the data, including in third countries. (…)

(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such (…) a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others.

(34) Any refusal or restriction of access should in principle be set out in writing to the data subject including the factual or legal reasons on which the decision is based.

(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the (…)national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question.

(36) A natural person should have the right to have inaccurate personal data concerning him or her rectified and the right of erasure where the processing of such data is not in compliance with the provisions laid down in this Directive. Where the personal data are processed in the course of a criminal investigation and proceedings, (…) the exercise of the rights of information, access, rectification, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

(37) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate measures and be able to demonstrate (…) the compliance of processing activities with the rules adopted pursuant to this Directive.

(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to be able to demonstrate compliance with the provisions adopted pursuant to this Directive, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes (…) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(40) Processing activities should be recorded by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring processing operations.

(41) In order to ensure effective protection of the rights and freedoms of data subjects (…) the controller or processor should consult with the supervisory authority in certain cases prior to intended processing.

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in severe material or moral harm (…) to the individual concerned. Therefore, as soon as the controller becomes aware that (…) a personal data breach has occurred which may result in severe material or moral harm, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose personal data (…) could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions (…).

(43) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it. Likewise, the communication to the data subject is not required if the controller has taken subsequent measures which ensure that rights and freedoms of affected data subjects are no longer likely to be severely affected (…).

(44) (…) A person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several public authorities or bodies, taking into account of their organisational structure and size (…). Such data protection officers must be in a position to perform their duties and tasks in an independent (…) manner.

(45) Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced.

(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how a given third country respects the rule of law, access to justice, as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law.

(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards or on the basis of a derogation laid down in the Directive.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. By way of derogation, in specific situations where no adequacy decision or appropriate safeguards exist, a transfer could take place if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.

(49a) Where personal data are transferred from a Member State to third countries or international bodies, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent public authority should be able to transfer the relevant personal data to the third country concerned without such prior authorisation.

(…)

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(52) Member States may entrust a supervisory authority already established (…) under Regulation (EU)…./2012 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with (…) financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

(54) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government or the head of state of the Member State (…).

(55) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be limited to (…) judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.

(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same duties and effective powers in each Member State, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. The investigative powers should include powers of access to data forming the subject matter of processing operations, access to any premises, including to any data processing equipment and means, and powers to collect all the information necessary for the performance of its supervisory duties. These powers should be exercised in conformity with Union law or Member State law. The powers of intervention should include 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 drawing a matter to the attention of national parliaments or other political institutions.

(57) Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

(58) The supervisory authorities should assist one another in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(59) The European Data Protection Board established by Regulation (EU)…./2012 should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.

(60) Every data subject should, without prejudice to any other administrative or non-judicial remedy, have the right to lodge a complaint with a supervisory authority (…) and have the right to a judicial remedy if they consider that their rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(61) Any body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of a data subject if duly mandated by him or her (…).

(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them.(…).

(…)

(64) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.

(…)

(67) In order to ensure uniform conditions for the implementation of this Directive as regards (…) the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[1].

(68) The examination procedure should be used for the adoption of measures as regards (…) the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, given that those acts are of general scope.

(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent public authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

---

1 OJ L 55, 28.2.2011, p. 13.

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.

(72) Specific provisions with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. The Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive (…), and which are in compliance with the relevant and applicable Union law prior to the entry into force of this Directive, should remain in force until amended, replaced or revoked. To the extend that such agreements are not compatible with Union law, Member States are required to take all appropriate steps to eliminate any incompatibilities (…).

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.[1]

[1] OJ L 335, 17.12.2011, p. 1.

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland shall not be bound by the rules laid down in this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by this Directive or subject to its application. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[1].

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[2].

---

1 OJ L 176, 10.7.1999, p. 36.
2 OJ L 53, 27.2.2008, p. 52.

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[1].

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.

---

1 OJ L 160 of 18.6.2011, p. 19.

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintainance of public order,] or the execution of criminal penalties.

2. In accordance with this Directive, Member States shall:

   (a) protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data; and

   (b) ensure that the exchange of personal data by competent public 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.

Article *2*

Scope

1. This Directive applies to the processing of personal data by competent public authorities for the purposes referred to in Article 1(1).

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. This Directive shall not apply to the processing of personal data:

   (a) in the course of an activity which falls outside the scope of Union law; (…)

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

Article 3

Definitions

For the purposes of this Directive:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

(…)

(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, combination (…) or (…) erasure;

(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(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;

(6) 'controller' means the competent public authority which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) 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;

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(8) 'recipient' means a natural or legal person, public authority, agency or any other body other than the data subject, the controller or the processor to which the personal data are disclosed;

(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;

(10) 'genetic data' means all personal data, (…) relating to the genetic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means (…) data related to the physical or mental health of an individual, which reveal information about his or her health status;

(12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to an individual;

(…)

(14) 'competent public authority' means any authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(15) 'supervisory authority' means an independent public authority which is established by a Member State in accordance with Article 39.

CHAPTER II

PRINCIPLES

Article 4

Principles relating to personal data processing

1. Member States shall provide that personal data must be:

(a) processed (…) lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; (…)

(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;

(ee) processed in a manner that ensures appropriate security of the personal data.

(…)

2. The controller shall be responsible for compliance with paragraph 1.

Article 5

Distinction between different categories of data subjects

(…)

Article 6

Different degrees of accuracy and reliability of personal data

(…)

Article 7

Lawfulness of processing

1. Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary:

(a) for the performance of a task carried out by a competent public authority, based on Union law or Member State 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.

2. Member States shall provide that the controller may further process personal data for historical, statistical or scientific purposes, subject to appropriate safeguads for the rights and freedoms of data subjects.

Article 7a

Specific processing conditions

1. Member States shall provide that where Union law or the national law applicable to the transmitting competent public authority provides for specific conditions applicable in specific circumstances to the processing of personal data, the transmitting public authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

2. Member States shall provide that the transmitting public authority does not apply conditions pursuant to paragraph 1 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to the transmitting public authority.

Article 8

Processing of special categories of personal data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

   (a) the processing is authorised by Union law or Member State law which provides appropriate safeguards for the rights and freedoms of the data subjects; or

   (b) the processing is necessary to protect the vital interests of the data subject or of another person; or

   (c) the processing (…) is necessary for the prevention of an immediate and serious threat to public security.

Article 9

(…) Profiling (…)

1. Member States shall provide that a decision based solely on profiling which produces an adverse legal effect for the data subject or severely affects him or her (…) shall be prohibited unless authorised by a law which provides appropriate safeguards for the rights and freedoms of the data subject (…).

2. Profiling shall not be based on special categories of personal data referred to in Article 8(1), unless Article 8(2) applies and appropriate safeguards for the rights and freedoms of the data subjects are in place.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 10

Communication and modalities for exercising the rights of the data subject

1. (…)

2. Member States shall provide that the controller shall take appropriate measures to provide any information referred to in Articles 11 and 11a and any communication under Articles 12 and 15 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing or, where appropriate, electronically or by other means.

3. Member States shall provide that the controller takes all reasonable steps to provide the information referred to in Articles 11 and 11a and to facilitate the exercise of data subject rights under Articles 12 and 15 (…).

4. Member States shall provide that the controller informs the data subject about the follow-up given to his or her request without undue delay.

5. Member States shall provide that the information provided under Articles 11 and 11a and any communication under Articles 12, 15 and 29 shall be provided (…) free of charge. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character (…), the controller may refuse to act on the request. In that case, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request (…).

5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 12 and 15, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 11

Information to be provided where the data are collected from the data subject

1. Subject to Article 11b, Member States shall provide that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with *at least* the following information:

(a) the identity and the contact details of the controller and, if any, of the data protection officer;

(aa) whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data; and

(b) the purposes of the processing for which the personal data are intended;

(c) (…)

(d) (…)

(e) the right to lodge a complaint to a supervisory authority (…).

(f) (…)

(g) (…).

2. (…)

3. (…)

4. (…)

5. (…)

Article 11a

Information to be provided where the data have not been obtained from the data subject

1. *Subject to Article 11b, Member States shall provide that where personal data have not been obtained from the data subject, the controller shall provide the data subject with at least the following information:*

   (a) the identity and the contact details of the controller and, if any, of the data protection officer;

   (b) the categories of personal data concerned;

   (c) the purposes of the processing for which the personal data are intended;

   (d) the right to lodge a complaint to a supervisory authority.

2. The controller shall provide the information referred to in paragraph 1:

   (a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or

   (b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

Article 11b

Limitations to the rights of information

1. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to Article 11 and 11a to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:

   (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;

(e) to protect the rights and freedoms of others.

2. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.

Article 12

Right of access for the data subject

1. Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller at reasonable intervals and free of charge confirmation as to whether or not personal data relating to him or her are being processed, and where such personal data are being processed to obtain access to such data and the following information:

(a) the purposes of the processing;

(b) (…)

(c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular the recipients in third countries;

(d) where possible, the envisaged period for which the personal data will be stored;

(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;

(f) the right to lodge a complaint to a supervisory authority (…);

(g) (…)

1a. Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.

2. (…)

Article 13

Limitations to the right of access

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

(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 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 (…) of any refusal or restriction of access, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy]. This shall not apply (…) 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

Additional modalities for exercising the right of access

1. Member States shall provide for the right of the data subject to request, 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. (…)

Article 15

Right to rectification, erasure and restriction of processing

1. Having regard to the nature and purpose of the processing concerned, Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to him or her which are inaccurate and (…) the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

1a. *Member States shall provide for the obligation of the controller to erase personal data without undue delay and of the right of the data subject to obtain from the controller the erasure of personal data (…) without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.*

1b. Member States shall provide for the right of the data subject to obtain from the controller the restriction of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data, or where they are required by the data subject for the establishment, exercise or defence of legal claims.

2. Member States shall provide that the controller informs the data subject (…) of any refusal of rectification, erasure or restriction of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy].

3. Member States shall provide that in the cases referred to in paragraphs 1, 1a and 1b the controller shall notify the recipients and that the recipients shall rectify, erase or restrict the processing of the personal data under their responsibility.

Article 16
Right to erasure

(…)

Article 17

Rights of the data subject in criminal investigations and proceedings

Member States may provide that the exercise of the rights (…) referred to in Articles 11, 11a, 12 and 15 is 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.

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1

GENERAL OBLIGATIONS

Article 18

Obligations of the controller

1. Member States shall provide that the controller implements appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.

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

2. (…)

Article 19

Data protection by design and by default

1. Member States shall provide that, having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, 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 protect the rights of the data subject.

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.

Article 20

Joint controllers

Member States shall provide that where a controller determines the purposes (…) 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, unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

Article 21

Processor

1. Member States shall provide that the controller shall use only (…) processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive (…).

2. Member States shall provide that the carrying out of processing by a processor shall 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 (…).

3. (…)

Article 22

Processing under the authority of the controller and processor

(…)

Article 23

Records of categories of personal data processing activities

1. Member States shall provide that each controller and processor shall maintain a record of all processing systems (…) under their responsibility.

2. (…)

3. The controller and the processor shall make such records available, on request, to the supervisory authority.

Article 24

Logging

1. Member States shall ensure that logs are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure in automated processing systems. The logs of consultation and disclosure shall show (…) the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.

2. The logs shall be used (...) for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.

Article 25

Cooperation with the supervisory authority

(…)

Article 26

Prior consultation of the supervisory authority

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:

(a) special categories of personal data referred to in Article 8 are to be processed;

(b) the type of processing, in particular where using new technologies, mechanisms or procedures, involves specific risks for the (…) rights and freedoms (…) of data subjects.

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.

3. Member States shall provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller. This period may be extended for a further month, taking into account the complexity of the intended processing.

SECTION 2

DATA SECURITY

Article 27

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, Member States shall provide that the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to these risks (…).

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:

   (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

   (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

   (d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

   (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);

   (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);

(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).

3. (…)

Article 28

Notification of a personal data breach to the supervisory authority

1. Member States shall provide that in the case of a personal data breach <u>which is likely to severely affect the rights and freedoms of data subjects</u>, the controller notifies, without undue delay (…) the personal data breach to the supervisory authority (…).

<u>1a</u>. <u>The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b).</u>

2. The processor shall alert and inform the controller <u>without undue delay</u> after having become aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least <u>describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or proposed to be taken by the controller to address the personal data breach</u>. (…)

4. Member States shall provide that the controller documents any personal data breaches referred to in paragraph 1, 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. (…)

6. (…)

Article 29

Communication of a personal data breach to the data subject

1. Subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to severely affect the rights and freedoms (…) 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.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach (…).

3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if:

   (a) the controller (…) has implemented appropriate technological protection measures, and those measures were applied to the personal data affected by the personal data breach in particular those that render the data unintelligible to any person who is not authorised to access it; or

   (b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or

   [(c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.]

4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted on the grounds referred to in Article 11b.

SECTION 3

DATA PROTECTION OFFICER

Article 30

Designation of the data protection officer

1. Union law or Member State law may provide that the controller or the processor designates a data protection officer.

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.

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

4. *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.*

5. *The controller or processor shall ensure that the data protection officer is provided with the means to perform (…) the tasks referred to under Article 32 effectively and can act in an independent manner with respect to the performance of his or her tasks (…).*

Article 31

Position of the data protection officer

(…)

Article 32

Tasks of the data protection officer

Member States shall provide that the controller or the processor entrusts the data protection officer (…) with the following tasks:

(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive (…);

(b) to monitor compliance with provisions adopted pursuant to this Directive and with (…) the policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related audits;

(c) (…)

(d) (…)

(e) (…)

(f) (…)

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on his or her own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data and consult, (…) as appropriate, on any other matter (…).

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 33

General principles for transfers of personal data

Member States shall provide that any transfer of personal data by competent public authorities (…) 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:

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and

(b) (…)

(c) the controller in the third country or international organisation is an authority competent for the purposes referred to in Article 1(1); and

(d) in case personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in compliance with its national law; and

(e) the Commission has decided pursuant to Article 34 that the third country or international organisation in question ensures an adequate level of protection or where appropriate safeguards are adduced or exist in accordance with Article 35.

Article 34

Transfers with an adequacy decision

1. Member States shall provide that a transfer of personal data to a recipient or recipients in 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 specific authorisation.

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:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, data protection rules (…) including concerning public security, defence, national security and criminal law as well as the security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation; as well as the existence of effective and enforceable data subject rights and (…) effective administrative and judicial redress for data subjects (…) whose personal data are being transferred;

   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility (…) for ensuring compliance with the data protection rules, for assisting and advising (…) data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

   (c) the international commitments the third country or international organisation concerned has entered into in relation to the protection of personal data.

3. The Commission after assessing the adequacy of the level of protection, 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. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2).

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3.

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 no longer ensures an adequate level of protection within the meaning of paragraph 2, and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The (…) implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(3). *At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision* (…).

6. Member States shall ensure that where a decision pursuant to paragraph 5 is taken, such decision (…) shall be without prejudice to transfers of personal data to the third country, or the territory or processing sector within that third country, or the international organisation in question pursuant to Articles 35 and 36 (…).

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 and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)

Article 35

Transfers by way of appropriate safeguards

1. (…) Member States shall provide that a transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where:

   (a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or

   (b) the controller (…) has assessed all the circumstances surrounding transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.

2. (…) Transfers under paragraph 1 (b) must be (…) documented and the documentation must be made available to the supervisory authority on request.

Article 36

Specific situations

(…) Member States shall provide that, in the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35, a transfer of personal data to a third country or an international organisation may take place only on condition that:

   (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

   (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

   (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

(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.

Article 36a

Transfers without prior authorisation by another Member State

Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) of Article 33 shall be permitted only if the transfer of the personal data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

Article 37

Specific conditions for the transfer of personal data

(…)

Article 38

International co-operation for the protection of personal data

(…)

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1

INDEPENDENT STATUS

Article 39

Supervisory authority

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive.

1a. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. (…) For this purpose, the supervisory authorities shall co-operate with each other and the Commission.

2. Member States may provide that a supervisory authority established (…) under Regulation (EU)…./2012 assumes responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which (…) shall represent those authorities in the European Data Protection Board.

Article 40

Independence

1. Member States shall ensure that each supervisory authority acts with complete independence in performing the duties and exercising the powers entrusted to it.

2. (…) Member States shall provide that the member or the members of the supervisory authority, in the performance of their duties, remain free from external influence, whether direct or indirect.

3. (…)

4. (…)

5. (…) Member States shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and exercise of its powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.

6 (…) Member States shall ensure that each supervisory authority must have its own staff which shall be appointed by and be subject to the direction of the member or the members of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate annual budgets which shall be made public.

Article 41

General conditions for the members of the supervisory authority

1. Member States shall provide that the member or the members of each supervisory authority must be appointed either by the parliament or the government or the head of state of the Member State concerned.

2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers.

3. (…)

4. (…)

5. (…)

Article 42

Rules on the establishment of the supervisory authority

Each Member State shall provide by law for:

(a) the establishment of each supervisory authority (…);

(b) (…)

(c) the rules and procedures for the appointment of the member or members of each supervisory authority (…);

(d) the duration of the term of the member or members of each supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;

(e) whether and, if so, for how many terms, the member or members of the supervisory authority shall be eligible for reappointment;

(f) the (…) conditions governing the employment of the member or members and staff of each supervisory authority and rules governing the cessation of employment.

(g) (…)

Article 43

Professional secrecy

Member States shall provide that the member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their duties or exercise of their powers, both during and after their term of office.

SECTION 2

DUTIES AND POWERS

Article 44

Competence

1. Member States shall provide that each supervisory authority shall be competent to perform the duties and to exercise (…) the powers conferred on it in accordance with this Directive on the territory of its own Member State.

2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of independent judicial bodies when acting in their judicial capacity.

Article 45

Duties

1. Member States shall provide that the supervisory authority:

   (a) monitors and enforces the application of the provisions adopted pursuant to this Directive and its implementing measures;

   (aa) promotes public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data;

   (ab) promotes the awareness of controllers and processors of their obligations under the provisions adopted pursuant to this Directive;

   (ac) upon request, provides information to any data subject concerning the exercise of his or her rights under the provisions adopted pursuant to this Directive and, if appropriate, co-operates with the supervisory authorities in other Member States to this end;

(b) deals with complaints lodged by any data subject, or by a body, organisation or association representing and duly mandated by that data subject in accordance with Article 50, and investigates, to the extent appropriate, the subject matter of the complaint and informs the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;

(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;

(d) provides mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of the provisions adopted pursuant to this Directive;

(e) conducts investigations on the application of the provisions adopted pursuant to this Directive either on its own initiative or on the basis of a complaint, or on request of another supervisory authority (…);

(f) monitors relevant developments insofar as they have an impact on the protection of personal data, in particular new technologies, mechanisms or procedures involving specific risks for the rights and freedoms of individuals;

(g) responds to consultation requests 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;

(h) gives advice on processing operations referred to in Article 26;

(i) contributes to the activities of the European Data Protection Board.

2. (…)

3. (…)

4. (…)

5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are manifestly unfounded or excessive, in particular due to their repetitive character, the supervisory authority may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 46

Powers

Member States shall provide that each supervisory authority shall have at least the following powers:

(a) investigative powers (…);

(b) effective powers of interventions (…);

(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 judicial or other relevant authorities.

Article 47

Activities report

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.

CHAPTER VII
CO-OPERATION

Article 48

Mutual assistance

1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions adopted pursuant to this Directive (…) 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 (…) inspections and investigations.

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority.

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.

Article 49

Tasks of the European Data Protection Board

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:

   (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

   (b) examine, on 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 (…) in order to encourage consistent application of those provisions;

   (c) review the practical application of guidelines, recommendations and best practices referred to in point (b) (…);

(d) give the Commission an opinion on the level of protection in third countries or international organisations;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(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;

(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice.

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.

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.

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.

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS

Article 50

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide that each supervisory authority shall deal with complaints lodged by any data subject (…) if he or she considers that the processing of personal data relating to him or her does not comply with provisions adopted pursuant to this Directive.

2. For the situation referred to in paragraph 1, Member States may provide for the right of any body, organisation or association which (…) has been properly constituted according to the law of a Member State to lodge the complaint with a supervisory authority on behalf of the data subject (…).

3. (…)

Article 51

Right to a judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority does not deal with the complaint (…) or does not inform the data subject within three months on the progress or outcome of the complaint lodged under Article 50.

(…)

Article 52

Right to a judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 50, Member States shall provide for the right of data subjects 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.

Article 53

Common rules for court proceedings

(…)

Article 54

Liability and the right to compensation

1. Member States shall provide that any person who has suffered damage as a result of (…) a processing operation which is non compliant 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.

2. Without prejudice to Article 20, 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.

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.

Article 55

Penalties

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

CHAPTER IX

(…) IMPLEMENTING ACTS

Article 56
Exercise of the delegation

(…)

Article 57

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER X
FINAL PROVISIONS

Article 58

Repeals

1. Council Framework Decision 2008/977/JHA is repealed.

2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 59

Relationship with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation

The specific provisions for the protection of personal data with regard to the processing of personal data by competent public authorities for the purposes (…) referred to in Article 1(1) 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.

Article 60

Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain in force until amended, replaced or revoked. In accordance with the Treaties, to the extent that such agreements concluded by Member States are not compatible with Union law, the Member State or States concerned shall take all appropriate steps to eliminate the incompatibilities established.

Article 61

Evaluation

1. The Commission shall evaluate the application of this Directive.

2. The Commission shall review within five 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 public 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.

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.

Article 62

Implementation

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.

   They shall apply those provisions from xx.xx.201x [date/ two years after entry into force].

   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.

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.

Article 63

Entry into force and application

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

Article 64

Addressees

This Directive is addressed to the Member States.