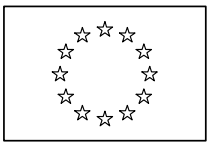

EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 10 final

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

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

This explanatory memorandum further details the approach for the new legal framework for the protection of personal data in the EU as presented in Communication COM (2012) 9 final. The legal framework consists of two legislative proposals:

– a proposal for a Regulation 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), and

– a 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.

This explanatory memorandum concerns the latter legislative proposal.

The centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC[1], was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by several instruments providing specific data protection rules in the area of police and judicial co-operation in criminal matters[2] (ex-third pillar), including Framework Decision 2008/977/JHA[3].

The European Council invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives[4]. In its resolution on the Stockholm Programme, the European Parliament[5] welcomed a comprehensive data protection scheme in the EU and among others called for the revision of the Framework Decision. The Commission stressed in its Action Plan implementing the Stockholm Programme[6] the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. The Action Plan underlined that *"in a global society characterised by rapid technological change where information exchange knows no borders, it is particularly important that privacy must be preserved. The Union must ensure that the fundamental right to data protection is consistently applied. We need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations."*

---

1 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, OJ L 281/95, p.31.

2 See the full list in Annex 3 to the Impact Assessment (SEC(2012)72).

3 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

4 In the Stockholm Programme, OJ C 115, 4.5.2010, p. 1.

5 See the Resolution of the European Parliament on the Stockholm Programme adopted on 25 November 2009.

6 COM(2010)171final.

In its Communication on "A comprehensive approach on personal data protection in the European Union"[7], the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.

Framework Decision 2008/977/JHA has a limited scope of application, since it only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. This is liable to create difficulties for police and other competent authorities in the areas of judicial co-operation in criminal matters and police co-operation. They are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage(see Section 2 below). Moreover, because of its nature and content, the Framework Decision leaves a large room for manoeuvre to Member States' national laws in implementing its provisions. Additionally, it does not contain any mechanism or advisory group similar to the Article 29 Working Party supporting common interpretation of its provisions, nor foresees any implementing powers for the Commission to ensure a common approach in its implementation.

Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) establishes the principle that everyone has the right to the protection of personal data. Moreover, with Article 16 (2) TFEU, the Lisbon Treaty introduces a specific legal basis for the adoption of rules on the protection of personal data that also applies to judicial co-operation in criminal matters and police co-operation. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right. Article 16 TFEU requires the legislator to lay down rules relating to the protection of individuals with regard to the processing of personal data also in the areas of judicial co-operation in criminal matters and police co-operation, covering both cross-border and domestic processing of personal data. This will allow protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, ensuring at the same time the exchange of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This will contribute to facilitating the co-operation in the fight against crime in Europe.

Due to the specific nature of the field of police and judicial co-operation in criminal matters it was acknowledged in Declaration 21[8] 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 TFEU may prove necessary.

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

This initiative is the result of extensive consultations with all major stakeholders on a review of the existing legal framework for the protection of personal data, which included two phases of public consultation:

---

7 European Commission, Communication on "A comprehensive approach on personal data protection in the European Union", COM(2010)609 final, 4 November 2010.

8 Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13.12.2007).

– From 9 July to 31 December 2009, the *Consultation on the legal framework for the fundamental right to the protection of personal data*. The Commission received 168 responses, 127 from individuals, business organisations and associations and 12 from public authorities. The non-confidential contributions can be consulted on the Commission's website[9].

– From 4 November 2010 to 15 January 2011, the *Consultation on the Commission's comprehensive approach on personal data protection in the European Union*. The Commission received 305 responses, of which 54 from citizens, 31 from public authorities and 220 from private organisations, in particular business associations and non-governmental organisations. The non-confidential contributions can be consulted on the Commission's website[10].

Whereas those consultations focused largely on the review of Directive 95/46/EC, targeted consultations were conducted with law enforcement stakeholders; in particular, a workshop was organised on 29 June 2010 with Member States' authorities on the application of data protection rules to public authorities, including in the area of police co-operation and judicial co-operation in criminal matters. Furthermore, on 2 February 2011, the Commission convened a workshop with Member States' authorities to discuss the implementation of Framework Decision 2008/977/JHA and, more generally, data protection issues in the area of police co-operation and judicial co-operation in criminal matters.

EU citizens were consulted through a Eurobarometer survey held in November-December 2010[11]. A number of studies were also launched.[12] The "Article 29 Working Party"[13] provided several opinions and useful input to the Commission[14]. The European Data Protection Supervisor also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication.[15]

The European Parliament approved by its resolution of 6 July 2011 a report that supported the Commission's approach to reforming the data protection framework.[16] The Council of the

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

11 Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

12 See the *Study on the economic benefits of privacy enhancing technologies* or the *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, January 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

13 The Working Party was set up in 1996 (by Article 29 of the Directive) with advisory status and composed of representatives of national Data Protection Supervisory Authorities (DPAs), the European Data Protection Supervisor (EDPS) and the Commission. For more information on its activities see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

14 See in particular the following opinions: on the "Future of Privacy" (2009, WP 168); on the concepts of "controller" and "processor" (1/2010, WP 169); on online behavioural advertising (2/2010, WP 171); on the principle of accountability (3/2010, WP 173); on applicable law (8/2010, WP 179); and on consent (15/2011, WP 187). Upon the Commission's request, it adopted also the three following Advice Papers: on notifications, on sensitive data and on the practical implementation of Article 28(6) of the Directive 95/46/EC. They can all be accessed at: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

15 Available on the EDPS website: http://www.edps.europa.eu/EDPSWEB/.

16 EP resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 (rapporteur: MEP Axel Voss (EPP/DE).

European Union adopted conclusions on 24 February 2011 in which it broadly supports the Commission's intention to reform the data protection framework and agrees with many elements of the Commission's approach. The European Economic and Social Committee likewise supported the Commission's general thrust to ensure a more consistent application of EU data protection rules across all Member States and an appropriate revision of the Directive 95/46/EC.[17]

In line with its “Better Regulation” policy, the Commission conducted an impact assessment of policy alternatives[18]. The impact assessment was based on the three policy objectives of improving the internal market dimension of data protection, making the exercise of data protection rights by individuals more effective and creating a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters. As regards this latter objective in particular, two policy options were assessed: a first one basically extending the scope of data protection rules in this area and addressing the gaps and other issues raised by the Framework Decision, and a second more far-reaching one with very prescriptive and stringent rules, which would also entail the immediate amendment of all other "former third pillar" instruments. A third "minimalistic" option based largely on interpretative Communications and policy support measures, such as funding programmes and technical tools, with minimum legislative intervention, was not considered appropriate to address the issues identified in this area in relation to data protection.

According to the Commission's established methodology, each policy option was assessed, with the help of an inter-service steering group, against its effectiveness to achieve the policy objectives, its economic impact on stakeholders (including on the budget of the EU institutions), its social impact and effect on fundamental rights. Environmental impacts were not observed.

The analysis of the overall impact led to the development of the preferred policy option which is incorporated in the present proposal. According to the assessment, its implementation will lead to further strengthening data protection in this policy area in particular by including domestic data processing, thereby also enhancing legal certainty for competent authorities in the areas of judicial co-operation in criminal matters and police co-operation.

The Impact Assessment Board (IAB) delivered an opinion on the draft impact assessment on 9 September 2011. Following the IAB’s opinion, in particular the following changes were made to the impact assessment:

– The objectives of the current legal framework (to what extent they were achieved and to what extent they were not), as well as the objectives of the envisaged reform, were clarified;

– More evidence and additional explanations/clarifications were added to the problems' definition section.

The Commission also prepared an Implementation Report related to Framework Decision 2008/977/JHA, based on its Article 29(2), which is to be adopted as part of the present data

[17] CESE 999/2011.
[18] SEC(2012)72.

protection package[19]. The findings of the report, based on input from Member States, also fed into the preparation of the Impact Assessment.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal Basis

The proposal is based on Article 16(2) TFEU, which is a new, specific legal basis introduced by the Lisbon Treaty for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

The proposal aims to ensure a consistent and high level of data protection in this field, thereby enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and co-operation between police and judicial authorities.

3.2. Subsidiarity and proportionality

According to the principle of subsidiarity (Article 5(3) TEU), action at Union level shall be taken only if and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union. In the light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action in the areas of police and criminal justice on the following grounds:

– The right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights and in Article 16(1) TFEU, requires the same level of data protection throughout the Union. It requires the same level of protection for data exchanged and data processed at domestic level.

– There is a growing need for law enforcement authorities in Member States to process and exchange at rapidly increasing rates for the purposes of preventing and combating transnational crime and terrorism. In this context, clear and consistent rules on data protection at EU level will help fostering co-operation between such authorities.

– In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which need to be organised at EU level to ensure unity of application of Union law. In certain situations, the EU is best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries.

– Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU.

[19] COM(2012)12.

– The proposed EU legislative action is likely to be more effective than similar actions at the level of Member States because of the nature and scale of the problems, which are not confined to the level of one or several Member States.

The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal, from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.

A Directive is therefore the best instrument to ensure harmonisation at EU level in this area while at the same time leaving the necessary flexibility to Member States when implementing the principles, the rules and their exemptions at national level. Given the complexity of the current national rules for the protection of personal data processed in the area of police co-operation and judicial co-operation in criminal matters, and the objective of comprehensive harmonisation of these rules by way of this Directive, the Commission will need to request Member States to provide explanatory documents explaining the relationship between the components of the Directive and the corresponding parts of national transposition instruments in order to be able to carry out its task of overseeing the transposition of this Directive.

3.3. Summary of fundamental rights issues

The right to protection of personal data is established by Article 8 of the Charter on Fundamental Rights of the EU and Article 16 TFEU as well in Article 8 of the ECHR. As underlined by the Court of Justice of the EU[20], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[21]. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected in Article 1(1) of Directive 95/46/EC, which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Other potentially affected fundamental rights enshrined in the Charter are the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24) and the right to an effective remedy before a tribunal and a fair trial (Article 47).

3.4. Detailed explanation of the proposal

3.4.1. CHAPTER I – GENERAL PROVISIONS

Article 1 defines the subject matter of the Directive, i.e. rules relating to processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and sets out the Directive's two-fold objective, i.e. to protect the fundamental rights and freedoms of natural persons and in

---

20 Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

21 In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union.

Article 2 defines the scope of application of the Directive. The scope of the Directive is not limited to cross-border data processing but applies to all processing activities carried out by 'competent authorities' (as defined in Article 3(14)) for the purposes of the Directive. The Directive applies neither to processing in the course of an activity which falls outside the scope of Union law, nor to processing by Union institutions, bodies, offices and agencies, which is subject to Regulation (EC) No 45/2001 and other specific legislation.

Article 3 contains definitions of terms used in the Directive. While some definitions are taken over from Directive 95/46/EC and Framework Decision 2008/977/JHA, others are modified, complemented with additional or newly introduced elements. New definitions are those of 'personal data breach', 'genetic data' and 'biometric data', 'competent authorities' (based on Article 87 TFEU and Article 2(h) of Framework Decision 2008/977/JHA) and, of a 'child', based on the UN Convention on the Rights of the Child[22].

3.4.2. CHAPTER II – PRINCIPLES

Article 4 sets out the principles relating to processing of personal data reflecting Article 6 of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA, while adjusting them to the particular context of this Directive.

Article 5 requires the distinction, as far as possible; between personal data of different categories of data subjects. This is a new provision, included neither in Directive 95/46/EC nor in Framework Decision 2008/977/JHA, but which had been proposed by the Commission in its original proposal for the Framework Decision[23]. It is inspired by the Council of Europe's Recommendation No R (87)15. Similar rules already exist for Europol[24] and Eurojust[25].

Article 6 on different degrees of accuracy and reliability reflects principle 3.2 of Council of Europe Recommendation No R (87)15. Similar rules, as also included in the Commission's proposal for the Framework Decision, exist for Europol[26].

Article 7 sets out the grounds for lawful processing, when necessary for the performance of a task carried out by a competent authority based on national law, to comply with a legal obligation to which the data controller is subject, in order to protect the vital interests of the data subject or another person or to prevent an immediate and serious threat to public security. The other grounds for lawful processing in Article 7 of Directive 95/46/EC are not appropriate for the processing in the area of police and criminal justice.

Article 8 sets out a general prohibition of processing special categories of personal data and the exceptions from this general rule, building on Article 8 of Directive 95/46/EC and adding genetic data, following ECtHR case law[27].

---

22 Referred to also in Article 2 (a) of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1.

23 COM(2005) 475 final.

24 Article 14 Europol Decision 2009/371/JHA.

25 Article 15 Eurojust Decision 2009/426/JHA.

26 Article 14 Europol Decision 2009/371/JHA.

Article 9 establishes a prohibition of measures based solely on automated processing of personal data if not authorised by law providing appropriate safeguards, in line with Article 7 of Framework Decision 2008/977/JHA.

3.4.3. CHAPTER III - RIGHTS OF THE DATA SUBJECT

Article 10 introduces the obligation for Member States to ensure easily accessible and understandable information, inspired in particular by principle 10 of the Madrid Resolution on international standards on the protection of personal data and privacy[28], and to oblige controllers to provide procedures and mechanisms for facilitating the exercise of the data subject's rights. This includes the requirement that the exercise of the rights shall be in principle free of charge.

Article 11 specifies the obligation for Member States to ensure the information towards the data subject. These obligations are building on Articles 10 and 11 of Directive 95/46/EC, without separate articles differentiating whether the information is collected from the data subject or not, and enlarging the information to be provided. It lays down exemptions from the obligation to inform, when such exemptions are proportionate and necessary in a democratic society for the exercise of the tasks of competent authorities (inspired by Article 13 of Directive 95/46/EC and Article 17 Framework Decision 2008/977/JHA).

Article 12 provides the obligation for Member States to ensure the data subject's right of access to their personal data. It follows Article 12(a) of Directive 95/46/EC, adding new elements for the information of the data subjects (on the storage period, their rights to rectification, erasure, or restriction and to lodge a complaint).

Article 13 provides that Member States may adopt legislative measures restricting the right of access if required by the specific nature of data processing in the areas of police and criminal justice, and on the information of the data subject on a restriction of access, following Article 17(2) and (3) of Framework Decision 2008/977/JHA.

Article 14 introduces the rule that in cases where direct access is restricted, the data subject must be informed on the possibility of indirect access via the supervisory authority, which should exercise the right on their behalf and must inform the data subject on the outcome of its verifications.

Article 15 on the right to rectification follows Article 12(b) of Directive 95/46/EC, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA.

Article 16 on the right to erasure follows Article 12(b) of Directive 95/46, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA. It integrates also the right to have the processing marked in certain cases, replacing the ambiguous terminology "blocking", used by Article 12(b) of Directive 95/46/EC and Article 18(1) of Framework Decision 2008/977/JHA.

Article 17 on the rectification, erasure and restriction of processing in judicial proceedings provides clarification based on Article 4(4) of Framework Decision 2008/977/JHA.

---

[27] ECtHR, judgment of 4.12.2008, S. and Marper v. UK (Application nos. 30562/04 and 30566/04).

[28] Adopted by the International Conference of Data Protection and Privacy Commissioners on 5.11.2009.

3.4.4. CHAPTER IV - CONTROLLER AND PROCESSOR

3.4.4.1. SECTION 1 GENERAL OBLIGATIONS

Article 18 describes the responsibility of the controller to comply with this Directive and to ensure compliance, including the adoption of policies and mechanisms for ensuring compliance.

Article 19 sets out that the Member States must ensure the compliance of the controller with the obligations arising from the principles of data protection by design and by default.

Article 20 on joint controllers clarifies the status of joint controllers as regards their internal relationship.

Article 21 clarifies the position and obligation of processors, following partly Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor that processes data beyond the controller's instructions is to be considered a co-controller.

Article 22 on processing under the authority of the controller and processor follows Article 16 of Directive 95/46/EC.

Article 23 introduces the obligation for controllers and processors to maintain documentation of all processing systems and procedures under their responsibility.

Article 24 concerns the keeping of records, in line with Article 10(1) of Framework Decision 2008/977, whilst providing further clarifications.

Article 25 clarifies the obligations of the controller and the processor regarding co-operation with the supervisory authority.

Article 26 concerns the cases where consultation with the supervisory authority is mandatory prior to the processing, based on Article 23 of Framework Decision 2008/977/JHA.

3.4.4.2. SECTION 2 DATA SECURITY

Article 27 on the security of processing is based on the current Article 17(1) of Directive 95/46 on the security of processing, and Article 22 of Framework Decision 2008/977/JHA, extending the related obligations to processors, irrespective of their contract with the controller.

Articles 28 and 29 introduce an obligation to notify personal data breaches, inspired by the personal data breach notification in Article 4(3) of the e-Privacy Directive 2002/58/EC, clarifying and separating the obligations to notify the supervisory authority (Article 28) and to communicate, in qualified circumstances, to the data subject (Article 29). Article 29 also provides for exemptions by referring to Article 11(4).

3.4.4.3. SECTION 3 DATA PROTECTION OFFICER

Article 30 introduces an obligation for the controller to appoint a mandatory data protection officer who should fulfil the tasks listed in Article 32. Where several competent authorities are acting under the supervision of a central authority, functioning as controller, at least this central authority should designate such a data protection officer. Article 18(2) of Directive

95/46/EC provided the possibility for Member States to introduce such requirement as a surrogate to the general notification requirement of that Directive.

Article 31 sets out the standing of the data protection officer.

Article 32 provides the tasks of the data protection officer.

3.4.5. *CHAPTER V - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS*

Article 33 sets out the general principles for data transfers to third countries or international organisations in the area of police co-operation and judicial co-operation in criminal matters, including onward transfers. It clarifies that transfers to third countries may take place only if the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties..

Article 34 lays down that transfers to a third country may take place in relation to which the Commission has adopted an adequacy decision under Regulation …./../201X or specifically in the area of police co-operation and judicial co-operation in criminal matters, or, in the absence of such decisions, where appropriate safeguards are in place. As long as adequacy decisions do not exist, the Directive ensures that transfers can continue to take place on the basis of appropriate safeguards and derogations. It furthermore sets out the criteria for the Commission's assessment of an adequate or not adequate level of protection, and expressly includes the rule of law, judicial redress and independent supervision. The article also provides for the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country. It introduces that a general adequacy decision adopted, following the procedures under Article 38 of the General Data Protection Regulation, shall be applicable within the scope of this Directive. Alternatively an adequacy decision can be adopted by the Commission exclusively for the purposes of this Directive.

Article 35 defines the appropriate safeguards needed prior to international transfers, in the absence of a Commission adequacy decision. These safeguards may be adduced by a legally binding instrument such as an international agreement. Alternatively, the data controller may on the basis of an assessment of the circumstances surrounding the transfer conclude that they exist.

Article 36 spells out the derogations for data transfer based on Article 26 of Directive 95/46/EC and Article 13 of Framework Decision 2008/977/JHA.

Article 37 obliges Member States to provide that the controller informs the recipient of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met by recipients of the personal data in the third country or international organisation.

Article 38 explicitly provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered offering an adequate level of protection, taking into account the OECD's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 June 2007.

CHAPTER VI - NATIONAL SUPERVISORY AUTHORITIES

3.4.5.1. SECTION 1 INDEPENDENT STATUS

Article 39 obliges Member States to establish supervisory authorities, following Article 28(1) of Directive 95/46/EC and Article 25 Framework Decision 2008/977/JHA, enlarging the mission of these authorities to contribute to the consistent application of the Directive throughout the Union, which may be the supervisory authority established under the General Data Protection Regulation.

Article 40 clarifies the conditions for the independence of supervisory authorities, implementing case law of the Court of Justice of the EU[29], inspired also by Article 44 of Regulation (EC) No 45/2001[30].

Article 41 provides general conditions for the members of the supervisory authority, implementing the relevant case law[31], inspired also by Article 42(2)-(6) of Regulation (EC) 45/2001.

Article 42 sets out rules on the establishment of the supervisory authority, including on conditions for its members, to be provided by the Member States by law.

Article 43 on professional secrecy of the members and staff of the supervisory authority follows Article 28(7) of Directive 95/46/EC and Article 25(4) Framework Decision 2008/977/JHA.

3.4.5.2. SECTION 2 DUTIES AND POWERS

Article 44 sets out the competence of the supervisory authorities, based on Article 28(6) of Directive 95/46/EC and Article 25(1) Framework Decision 2008/977/JHA. Courts, when acting in their judicial authority, are exempted from the monitoring by the supervisory authority, but not from the application of the substantive rules on data protection.

Article 45 provides the obligation of Member States to provide for the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public on risk, rules, safeguards and rights. A particular duty of the supervisory authorities in the context of this Directive is, where direct access is refused or restricted, to exercise the right of access on behalf of data subjects and to check the lawfulness of the data processing.

Article 46 provides the powers of the supervisory authority, based on Article 28(3) of Directive 95/46/EC, Article 25(2) and (3) of Framework Decision 2008/977/JHA.Article 47 obliges the supervisory authorities to draw up annual activity reports, based on Article 28(5) of Directive 95/46/EC.

---

29 Court of Justice of the EU, judgment of 9.3.2010, Commission / Germany (C-518/07, ECR 2010 p. I-1885)

30 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ L 008 , 12/.01/.2001, p.1.

31 Op. cit., footnote 27.

3.4.6. CHAPTER VII – CO-OPERATION

Article 48 introduces rules on mandatory mutual assistance whereas Article 28 (6)2 of Directive 95/46/EC provided simply a general obligation to co-operate, without specifying further.

Article 49 provides that the European Data Protection Advisory Board, established by the General Data Protection Regulation, exercises its tasks also in relation to processing activities within the scope of this Directive. In order to provide complementary support, the Commission will seek the advice of representatives of authorities competent for the prevention, investigation, detection and prosecution of criminal penalties of the Member States, as well as representatives of Europol and Eurojust, by means of an expert group on the law-enforcement related aspects of data protection.

3.4.7. CHAPTER VIII - REMEDIES, LIABILITY AND SANCTIONS

Article 50 provides the right of any data subject to lodge a complaint with a supervisory authority, based on Article 28(4) of Directive 95/46/EC, and relates to any infringement of the Directive in relation to the complainant. It also specifies the bodies, organisations or associations which may lodge a complaint on behalf of the data subject and also in case of a personal data breach independently of a data subject's complaint.

Article 51 concerns the right to a judicial remedy against a supervisory authority. It builds on the general provision of Article 28(3) of Directive 95/46/EC and provides specifically that the data subject may launch a court action for obliging the supervisory authority to act on a complaint.

Article 52 concerns the right to a judicial remedy against a controller or processor, based on Article 22 of Directive 95/46/EC and Article 20 of Framework Decision 2008/977/JHA.

Article 53 introduces common rules for court proceedings, including the rights of bodies, organisations or associations to represent data subjects before the courts, and the right of supervisory authorities to engage in legal proceedings. The obligation of Member States to ensure rapid court actions is inspired by Article 18(1) of the e-Commerce Directive 2000/31/EC[32].

Article 54 obliges Member States to provide for the right to compensation. It builds on Article 23 of Directive 95/46/EC and Article 19(1) of Framework Decision 2008/977/JHA, extends this right on damages caused by processors and clarifies the liability of co-controllers and co-processors.

Article 55 obliges Member States to lay down rules on penalties, to sanction infringements of the Directive, and to ensure their implementation.

---

[32] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'); OJ L 178, 17.7.2000, p. 1.

3.4.8. CHAPTER IX – DELEGATED ACTS AND IMPLEMENTING ACTS

Article 56 contains standard provisions for the exercise of delegations in line with Article 290 TFEU. This allows the legislator to delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts).

Article 57 contains the provision for the Committee procedure needed for conferring implementing powers on the Commission in cases where, in accordance with Article 291 TFEU, uniform conditions for implementing legally binding acts of the Union are needed. The examination procedure applies.

3.4.9. CHAPTER X – FINAL PROVISIONS

Article 58 repeals Framework Decision 2008/977/JHA.

Article 59 sets out that specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in Union acts, regulating the processing of personal data or the access to information systems within the scope of the Directive, and adopted prior to the adoption of this Directive, remain unaffected.

Article 60 clarifies the relationship of this Directive with previously concluded international agreements by Member States in the field of judicial co-operation in criminal matters and police co-operation.

Article 61 provides for the obligation of the Commission to evaluate and report on the implementation of the Directive, in order to assess the need to align the previously adopted specific provisions referred to in Article 59 with this Directive.

Article 62 sets out the obligation of the Member States to transpose the Directive in their national law and notify to the Commission the provisions adopted pursuant to the Directive.

Article 63 determines the date of the entry into force of the Directive.

Article 64 lays down the addressees of this Directive.

4. BUDGETARY IMPLICATIONS

The legislative financial statement accompanying the proposal for the General Data Protection Regulation covers the budgetary impacts for the Regulation and this Directive.

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 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[33],

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.

(2) The processing of personal data is designed to serve man; 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 authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

[33] OJ C… , p. .

(4) This requires facilitating the free flow of data between competent 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[34] 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[35] 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.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent 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 authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must 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 provides that the European Parliament and the Council should 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

---

34 OJ L 281, 23.11.1995, p. 31.

35 OJ L 350, 30.12.2008, p. 60.

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 authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences 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 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.

(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 technological neutral and not depend on the techniques 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, in particular concerning national security, or to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.

(16) The principles of 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. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(17) Personal data relating to health should include in particular all data pertaining to the health status of a data subject, information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or 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, e.g. 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 fair and lawful in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit.

(19) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent 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. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. Every reasonable step should be taken to ensure that 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 authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued.

(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should as far as possible be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals.

(24) As far as possible personal data should be distinguished 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 authorities.

(25) In order to be lawful, the processing of personal data should be necessary for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest by a competent authority based on 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.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights or privacy, including genetic data, deserve specific protection.

Such data should not be processed, unless processing is specifically authorised by a law which provides for suitable measures to safeguard the data subject's legitimate interests; or processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.

(27) Every natural person should have the right not to be subject to a measure which is based solely on automated processing if it produces an adverse legal effect for that person, unless authorised by law and subject to suitable measures to safeguard the data subject’s legitimate interests.

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

(29) Modalities should be provided for facilitating the data subject’s exercise of their rights under this Directive, including mechanisms to request, free of charge, in particular access to data, rectification and erasure. The controller should be obliged to respond to requests of the data subject without undue delay.

(30) The principle of fair processing requires that the data subjects should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure 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, in cases 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, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.

(32) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, 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, for what period, which recipients receive the data, including in third countries Data subjects should be allowed to receive a copy of their personal data which are being processed.

(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 partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned, 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 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 competent 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) Any person should have the right to have inaccurate personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the main principles laid down in this Directive. Where the personal data are processed in the course of a criminal investigation and proceedings,, rectification, the rights of information, access, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

(37) Comprehensive 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 ensure the compliance of processing operations 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 ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt 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, conditions 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 documented 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 this documentation available upon request, so that it might serve for monitoring processing operations. .

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

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in harm, including reputational damage to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without undue

delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of an individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the processing of personal data.

(43) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of misuse. Moreover, such rules and procedures should take into account the legitimate interests of competent authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(44) The controller or the processor should designate a person who would assist the controller or processor to monitor compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several entities of the competent authority. The data protection officers must be in a position to perform their duties and tasks independently and effectively.

(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 further 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 the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.

(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, does not offer 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 or processor 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. In cases where no grounds for allowing a transfer exist, derogations should be allowed 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.

(50) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(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 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 in Member States 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 adequate 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 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 of the Member State, and include rules on the personal qualification of the members and the position of those members.

(55) While this Directive applies also to the activities of national courts, 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 genuine 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.

(57) Each supervisory authority should hear 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 have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under 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 protects 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 data subjects if duly mandated by them, or to lodge, independently of a data subject's complaint, its own complaint where it considers that a personal data breach has occurred.

(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.

(63) Member States should ensure that court actions, in order to be effective, allow the rapid adoption of measures to remedy or prevent an infringement of this Directive.

(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.

(66) In order to fulfil 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 authorities within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of notifications of a personal data breach to the supervisory authority. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

(67) In order to ensure uniform conditions for the implementation of this Directive as regards documentation by controllers and processors, security of processing, notably in relation to encryption standards, notification of a personal data breach to the supervisory authority, and 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[36].

(68) The examination procedure should be used for the adoption of measures as regards documentation by controllers and processors, security of processing, notification of a personal data breach to the supervisory authority, and 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 does not 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 authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by

[36] OJ L 55, 28.2.2011, p. 13.

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

(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 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 relation 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 should be amended in line with this Directive.

(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.[37]

(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

[37] OJ L335, 17.12.2011, p. 1.

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[38].

(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[39].

(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[40].

(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.

---

38 OJ L 176, 10.7.1999, p. 36.
39 OJ L 53, 27.2.2008, p. 52.
40 OJ L 160 of 18.6.2011, p. 19.

HAVE ADOPTED THIS DIRECTIVE:

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 authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

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

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

   (b) ensure that the exchange of personal data by competent authorities within the Union 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 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, in particular concerning national security;

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

Article 3
Definitions

For the purposes of this Directive:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an

identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(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, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(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 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 data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) ‘data concerning health’ means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'child' means any person below the age of 18 years;

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

(15) 'supervisory authority' means a 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

Member States shall provide that personal data must be:

(a) processed fairly and 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed;

(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.

.

Article 5
Distinction between different categories of data subjects

1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal

offences, or a contact or associate to one of the persons mentioned in (a) and (b); and

(e) persons who do not fall within any of the categories referred to above.

Article 6
Different degrees of accuracy and reliability of personal data

1. Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.

2. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.

Article 7
Lawfulness of processing

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 authority, based on law for the purposes set out in Article 1(1); or

(b) for compliance with a legal obligation to which the controller is subject; or

(c) in order to protect the vital interests of the data subject or of another person; or

(d) for the prevention of an immediate and serious threat to public security.

Article 8
Processing of special categories of personal data

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

2. Paragraph 1 shall not apply where:

(a) the processing is authorised by a law providing appropriate safeguards; or

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

(c) the processing relates to data which are manifestly made public by the data subject.

Article 9

Measures based on profiling and automated processing

1. Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 10

Modalities for exercising the rights of the data subject

1. Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.

2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language.

3. Member States shall provide that the controller takes all reasonable steps to establish procedures for providing the information referred to in Article 11 and for the exercise of the rights of data subjects referred to in Articles 12 to 17.

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

5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are vexatious, in particular because of their repetitive character, or the size or volume of the request, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the vexatious character of the request.

Article 11

Information to the data subject

1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller takes all appropriate measures to provide the data subject with at least the following information:

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

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

(c) the period for which the personal data will be stored;

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

(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;

(f) the recipients or categories of recipients of the personal data, including in third countries or international organisations;

(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

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

(a) at the time when the personal data are obtained from the data subject, or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.

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

(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.

5. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 4.

Article 12
Right of access for the data subject

1. Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to them are being processed. Where such personal data are being processed, the controller shall provide the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

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

   (d) the 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 the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their source.

2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.

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 person 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 in writing on any refusal or restriction of access, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1.

4. Member States shall ensure that the controller documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based.

Article 14
Modalities for exercising the right of access

1. Member States shall provide for the right of the data subject to request, in particular in cases referred to in Article 13, that the supervisory authority checks the lawfulness of the processing.

2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.

3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

Article 15
Right to rectification

1. Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, in particular by way of a corrective statement.

2. Member States shall provide that the controller informs the data subject in writing on any refusal of rectification, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Article 16
Right to erasure

1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive.

2. The controller shall carry out the erasure without delay.

3. Instead of erasure, the controller shall mark the personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the personal data have to be maintained for purposes of proof;

(c) the data subject opposes their erasure and requests the restriction of their use instead.

4. Member States shall provide that the controller informs the data subject in writing of any refusal of erasure or marking of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Article 17
Rights of the data subject in criminal investigations and proceedings

Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 18
Responsibility of the controller

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

2. The measures referred to in paragraph 1 shall in particular include:

(a) keeping the documentation referred to in Article 23;

(b) complying with the requirements for prior consultation pursuant to Article 26;

(c) implementing the data security requirements laid down in Article 27;

(d) designating a data protection officer pursuant to Article 30.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.

Article 19

Data protection by design and by default

1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.

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, conditions and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Article 21

Processor

1. Member States shall provide that where a processing operation is carried out on behalf of a controller, the controller must choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.

2. Member States shall provide that the carrying out of processing by a processor must be governed by a legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited.

3. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 20.

Article 22

Processing under the authority of the controller and processor

Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.

Article 23
Documentation

1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.

2. The documentation shall contain at least the following information:

   (a) the name and contact details of the controller, or any joint controller or processor;

   (b) the purposes of the processing;

   (c) the recipients or categories of recipients of the personal data;

   (d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation.

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

Article 24
Keeping of records

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

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

Article 25
Cooperation with the supervisory authority

1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing all information necessary for the supervisory authority to perform its duties.

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

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 data referred to in Article 8 are to be processed;

   (b) the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

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.

SECTION 2
DATA SECURITY

Article 27
Security of processing

1. Member States shall provide that the controller and the processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

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. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

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, the controller notifies, without undue delay and, where feasible, not later than 24 hours after having become aware of it, the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases where the notification is not made within 24 hours.

2. The processor shall alert and inform the controller immediately after having become aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the possible consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

Article 29

Communication of a personal data breach to the data subject

1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 28(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

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

SECTION 3
DATA PROTECTION OFFICER

Article 30

Designation of the data protection officer

1. Member States shall 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. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.

Article 31
Position of the data protection officer

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

2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.

Article 32
Tasks of the data protection officer

Member States shall provide that the controller or the processor entrusts the data protection officer at least 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 and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;

(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;

(d) to ensure that the documentation referred to in Article 23 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;

(f) to monitor the application for prior consultation to the supervisory authority, if required pursuant to Article 26 ;

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

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.

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 authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:

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

(b) the conditions laid down in this Chapter are complied with by the controller and processor.

Article 34
Transfers with an adequacy decision

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) …./2012 or in accordance with paragraph 3 of this Article that the third country or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

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, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law as well as the security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

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

(c) the international commitments the third country or international organisation in question has entered into.

3. The Commission may decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. The Commission may decide within the scope of this Directive that a third country or a territory or a processing sector within that third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 57(3).

6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.

8. The Commission shall monitor the application of the implementing acts referred to in paragraphs 3 and 5.

Article 35
Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a recipient in a third country or an international organisation may take place where:

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

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

1. The decision for transfers under paragraph 1 (b) must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request.

Article 36
Derogations

By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:

(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 37
Specific conditions for the transfer of personal data

Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met.

Article 38
International co-operation for the protection of personal data

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

(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 39
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.

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

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.

Article 40

Independence

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

2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

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

6 Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.

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

Article 41

General conditions for the members of the supervisory authority

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

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.

Article 42
Rules on the establishment of the supervisory authority

Each Member State shall provide by law:

(a) the establishment and status of the supervisory authority in accordance with Articles 39 and 40;

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;

(c) the rules and procedures for the appointment of the members of the supervisory authority, as well as the rules on actions or occupations incompatible with the duties of the office;

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

(e) whether the members of the supervisory authority shall be eligible for reappointment;

(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including where they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Article 43
Professional secrecy

Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

SECTION 2
DUTIES AND POWERS

Article 44
Competence

1. Member States shall provide that each supervisory authority exercises, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.

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

Article 45
Duties

1. Member States shall provide that the supervisory authority:

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

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

   (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 and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;

   (e) conducts investigations either on its own initiative or on the basis of a complaint, or on request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;

   (f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

   (g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

   (h) is consulted on processing operations pursuant to Article 26;

   (i) participates in the activities of the European Data Protection Board.

2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

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 vexatious, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action required by the data subject. The supervisory authority shall bear the burden of proving of the vexatious character of the request.

Article 46
Powers

Member States shall provide that each supervisory authority must in particular be endowed with:

(a) investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

(b) effective powers of intervention, such as the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller, or referring the matter to national parliaments or other political institutions ;

(c) the power to engage in legal proceedings where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of the judicial authorities.

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 pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.

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 addressed to the supervisory authorities 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) and report regularly to the Commission on these;

(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 for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.

2. Member States shall provide for the right of any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and is being properly constituted according to the law of a Member State to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data. The organisation or association must be duly mandated by the data subject(s).

3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Article 51
Right to a judicial remedy against a supervisory authority

1. Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.

2. Each data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).

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

Article 52

Right to a judicial remedy against a controller or processor

Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that 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

1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51 and 52 on behalf of one or more data subjects.

2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions adopted pursuant to this Directive or to ensure consistency of the protection of personal data within the Union.

3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

Article 54

Liability and the right to compensation

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

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
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 56
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 28(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.

3. The delegation of power referred to in Article 28(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 28(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or the Council.

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
Relation 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 authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.

Article 60
Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation

International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.

Article 61
Evaluation

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

2. The Commission shall review within three years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.

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.

Done at Brussels, 25.1.2012

For the European Parliament	*For the Council*
The President	*The President*