EUROPEAN COMMISSION

Brussels, XXX
[…](2011) XXX draft

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

("Police and Criminal Justice Data Protection Directive")

Version 34

(2011-11-29)

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)xxx 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 (Police and Criminal Justice Data Protection Directive).

This explanatory memorandum concerns that second legislative proposal on data protection in the areas of police and criminal justice.

The centrepiece of existing EU legislation on 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 cooperation in criminal matters[2] (ex third pillar), including Framework Decision 2008/977/JHA[3].

Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.

Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies. Personal data protection therefore plays a central role in the Digital Agenda for Europe[4], and more generally in the Europe 2020 Strategy[5].

---

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.

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 COM(2010)245 final.

5 COM(2010)2020 final.

The Lisbon Treaty defines the right to personal data protection as a principle of the EU and introduces a specific legal basis for the adoption of rules on the protection of personal data[6] that also applies to police and judicial cooperation in criminal matters. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right.

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[7]. In its resolution on the Stockholm Programme, the European Parliament[8] 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[9] the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies.

In its Communication on "A comprehensive approach on personal data protection in the European Union"[10], the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.

The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity[11]. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.

Framework Decision 2008/977/JHA however 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 creates a practical difficulty for police and other authorities who are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain data may become the object of a cross-border exchange at a later stage[12]. The Framework Decision also leaves a very large room for manoeuvre to Member States' national laws in implementing its provisions, leading to varying standards that affect the efficiency of law enforcement cooperation.

The Lisbon Treaty defines the right to data protection as a principle of the EU and introduces a specific legal basis for the adoption of rules on the protection of personal data[13] that also applies to police and judicial cooperation in criminal matters. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right. It

---

6 Article 16 of the Treaty on the Functioning of the European Union (TFEU).

7 In the Stockholm Programme - OJ C115, 4 May 2010.

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

9 COM(2010)171final.

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

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 ("*EB 2011" in future references*).

12 This was confirmed by several Member States when replying to the Commission's questionnaire in relation to the Implementation Report on the Framework Decision (COM(2012)…).

13 Article 16 of the Treaty on the Functioning of the European Union (TFEU).

provides therefore the legal basis for rules relating to the protection of individuals with regard to the processing of personal data also in the areas of police and criminal justice, aiming to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and for ensuring 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 facilitate the cooperation in the fight against crime in Europe. The new legal basis in Article 16 TFEU aims for a consistent and coherent approach on personal data protection in the Union and covers thus both cross-border and domestic processing of personal data by the competent authorities in the area of police and criminal justice.

Due to the specific nature of the field of police and judicial cooperation in criminal matters it was acknowledged in Declaration 21[14] to the TEU that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police 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:

– 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[15].

– 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[16].

Targeted consultations were also conducted with key 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 cooperation and judicial cooperation 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 cooperation and judicial cooperation in criminal matters.

---

14 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).

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

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

EU citizens were consulted through a Eurobarometer survey held in November-December 2010[17]. A number of studies were also launched.[18] The "Article 29 Working Party"[19] provided several opinions and useful input to the Commission[20]. The European Data Protection Supervisor also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication.[21]

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.[22] The Council of the 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 to may elements of the Commission's approach. The European Economic and Social Committee equally supported an appropriate revision of the Data Protection Directive and the Commission's general thrust to ensure a more consistent application of EU data protection rules across all Member States.[23]

In line with its "Better Regulation" policy, the Commission conducted an impact assessment of policy alternatives. 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 cooperation in criminal matters. Three policy options of different degrees of intervention were assessed: the first option consisted of minimal legislative amendments and the use of interpretative Communications and policy support measures such as funding programmes and technical tools; the second option comprised a set of legislative provisions addressing each of the issues identified in the analysis and the third option was the centralisation of data protection at EU level through precise and detailed rules for all sectors and the establishment of an EU agency for monitoring and enforcement of the provisions.

According to the Commission's established methodology, each policy option was assessed, involving an Interservice steering group, against its effectiveness to achieve the policy

---

17 Cit. footnote 9.

18 In addition to the *Study on the economic benefits of privacy enhancing technologies* (cit., footnote 2), see also 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). A study for an impact assessment for the future EU legal framework for personal data protection is also ongoing.

19 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.

20 See in particular the following opinions: on the "Future of Privacy" (n° /2009, WP168); on the Concepts of "Controller" and Processor" (n° 1/2010, WP169); on Online Behavioural Advertising (n°2/2010, WP 171); on the Principle of Accountability (n° 3/2010, WP 173); on Applicable law (n° 8/2010, WP 179 – December 2010); and on consent. Upon the Commission's request, it adopted also the three following Advice Papers: on Notifications, on Sensitive Data and on Article 28(6) of the Data Protection Directive. They can all be retrieved at: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.

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

22 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).

23 CESE 999/2011.

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 *inter alia* to considerable improvements regarding legal certainty for data controllers and citizens, reduction of administrative burden, consistency of data protection enforcement in the Union, the effective possibility of individuals to exercise their data protection rights to the protection of personal data within the EU and the efficiency of data protection supervision and enforcement. Implementation of the preferred policy options are also expected to contribute to the Commission's objective of simplification and reduction of administrative burden and to the objectives of the Digital Agenda for Europe, the Stockholm Action Plan and the Europe 2020 strategy.

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 current reform, were clarified;

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

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.

A Directive is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the field of police and criminal justice and to cover processing both in the cross-border and domestic context.

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 cooperation 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 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.

– Personal data are transferred across national boundaries, both internal and external borders, at rapidly increasing rates. In addition, there are practical challenges to enforcing data protection legislation and a need for cooperation between Member States and their authorities, which need to be organised at EU level to ensure unity of application of Union law. The EU is also 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.

– The EU legislative actions proposed are 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 process from the identification and evaluation of alternative policy options to the drafting of this 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 and their exemptions at national level.

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 ECJ[24] , the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[25]. 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

---

[24] ECJ, judgment of 9.11.2010 in cases C-92/09 and 93/09, Schecke

[25] 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.

(Article 21); the rights of the child (Article 24) and the right to an effective remedy before a tribunal (Article 47).

3.4. Detailed explanation of the proposal

3.4.1. CHAPTER I – GENERAL PROVISIONS

Article 1 sets out the subject matter of the Directive, rules relating to processing for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and the its two-fold objective, 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 exchange of personal data between competent authorities within the Union.

Article 2 defines the scope of application of the Directive. Contrary to the Framework Decision 2008/977/JHA, 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(13)) for the purposes of the Directive. The Directive does neither apply 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 of Regulation (EC) No 45/2001 and of specific legislation.

Article 3 contains the definitions for terms used in the Directive. While some definitions are taken over from Directive 95/46/EC, others are modified, complemented with additional elements or newly introduced. New definitions are those of 'personal data breach', 'genetic data' and 'biometric data', 'competent authorities' (following Article 87 TFEU and Article 2(h) of Framework Decision 2008/977/JHA) and, 'of a child', following the UN Convention on the Rights of the Child[26].

3.4.2. CHAPTER II – PRINCIPLES

Article 4 sets out the principles relating to processing of personal data, insofar following Article 5 of the General Data Protection Regulation and reflecting Article 6 of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA. New elements are the expressly reference to the transparency principle, to the data minimisation principle and to the obligation to process only of non-personal data, as far as possible, as well as to the comprehensive responsibility and liability of the controller, responding to the debate on a 'principle of accountability'. Furthermore, this Article lays down the conditions for the access of competent authorities to data processed by other controllers and the requirements for the the quality of legislation applying to the processing of personal data within the scope of this Directive, building in particular on the relevant case law of the European Court of Human Rights (ECtHR) related to . In particular, the law must be clear and accessible.

Article 5 requires the distinction between personal data of different categories of data subjects is a new provision, included neither in Directive 95/46/EC nor in Framework Decision 2008/977/JHA (but had been proposed by the Commission in its proposal on the Framework

[26] Referred to also in the legislative proposals COM(2010)94final and COM(2011)275final.

Decision[27]). It is inspired by of the Council of Europe's Recommendation No R (87)15. Similar rules already exist for Europol[28] and Eurojust[29].

Article 6 on different degrees of accuracy and reliability reflects principle 3.2 of Recommendation No R (87)15. Similar rules, as also included in the Commission's proposal for the Framework Decision, exist for Europol[30].

Article 7 sets out the grounds for lawful processing sets out the criteria for lawful processing, when necessary for the performance of a task carried out by a competent authority, or in order to protect the vital interests of the data subject. 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 clarifies the conditions for the change of purpose of the processing, i.e. for another purpose than the one for which the personal data have been initially collected.

Article 9 sets out the general prohibition for processing special categories of personal data and the exceptions from this general rule, building insofar on Article 8 of Directive 95/46/EC.

Article 10 establishes rules on the processing of genetic data, "codifying" ECtHR case law[31].

Article 11 establishes a prohibition of measures based on profiling, if not authorised by law, following Article 7 of Framework Decision 2008/977/JHA.

3.4.3. CHAPTER III - RIGHTS OF THE DATA SUBJECT

Article 12 introduces the obligation for Member States to ensure transparent, 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[32], and to oblige controllers to provide procedures and mechanisms for facilitating the exercise of the data subject's rights. This includes means for electronic requests where the data are processed by automated means, an obligation for the controller to respond to the data subject's request within a defined a deadline and the requirement that the exercise of the rights shall be in principle free of charge.

Article 13 specifies the obligation of Member States to ensure the information towards the data subject. These obligations are based 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 (cf. Article 13 of Directive 95/46/EC), subject to a concrete and individual examination whether such restriction should apply in a specific case.

---

27 COM(2005)475 final.

28 Article 14 Europol Decision 2009/371/JHA.

29 Article 15 Eurojust Decision 2009/426/JHA.

30 Article 14 Europol Decision 2009/371/JHA.

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

32 Adopted by the International Conference of Data Protection and Privacy Commissioners on 5.11.2011.

Article 14 provides the obligation of 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 and to lodge a complaint).

Article 15 provides that Member States may adopt legislative measures restricting the right of access as required by 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 16 introduces the rule that in cases where direct access is restricted, the data subject must be informed on the possibility indirect access via the supervisory authority, which must inform the data subject on the outcome of its verifications.

Article 17 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 (cf. also principle 6.3 of CoE Police Recommendation (87)15.), spelt out, for reasons of clarity, in a separate article.

Article 18 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 restricted in certain cases, avoiding the ambiguous terminology "blocking", used by Article 12(b) of Directive 95/46/EC and Article 18(1) of Framework Decision 2008/977/JHA. It further provides that mechanisms must be in place for ensuring compliance with the obligation to erasure and a periodic review of stored data.

Article 19 on the rectification, erasure and restriction of processing in judicial proceedings provides clarification based on Article 4(4) of Framework Decision 2008/977/JHA.

3.4.4. CHAPTER IV - CONTROLLER AND PROCESSOR

3.4.4.1. SECTION 1 GENERAL OBLIGATIONS

Article 20, responding to the debate on a "principle of accountability", describes in detail the responsibility of the controller to comply with this Directive and to demonstrate compliance, including the adoption of policies and mechanisms for ensuring compliance.

Article 21 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 default.

Article 22 on joint controllers clarifies the status of joint controllers as regards their internal relationship and towards the data subject.

Article 23 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 24 on processing under the authority of the controller and processor follows Article 16 of Directive 95/46/EC.

Article 25 introduces the obligation for controllers and processors to maintain documentation of all processing operations under their responsibility, instead of a general notification to the supervisory authority required by Articles 18(1) and 19 of Directive 95/46/EC.

Article 26 concerns the keeping of records, cf. Article 10(1) of Framework Decision 2008/977, but strengthened in wording, inspired by Article 16 of Council Decision 2008/633/JHA.

Article 27 clarifies the obligations of the controller and the processor regarding cooperation with the supervisory authority.

3.4.4.2. SECTION 2 DATA SECURITY

Art. 28 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 the contract with the controller.

Articles 29 and 30 introduce an obligation to notify personal data breaches, inspired by the personal data breach notification in Article 4(3) of the ePrivacy Directive 2002/58/EC, clarifying and separating the obligations to notify the supervisory authority (Article 29) and to communicate, in qualified circumstances, to the data subject (Article 30).

3.4.4.3. SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 31 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations by relevant information systems or where the processing concerns procedures for the processing of personal data; it does thus not concern processing in individual cases. The list of such risky processing operations is not exhaustive, so as to ensure flexibility also in view of new developments.

Article 32 concerns the cases where consultation of, the supervisory authority is mandatory prior to the processing. The supervisory authority has certain flexibility in determining processing operations which it deems necessary for prior consultation. Other than the concept of prior checking in Article 20 of Directive 95/46/EC or of prior consultation in Article 23 of Framework Decision 2008/977/JHA, it is expressly laid down that the supervisory authority shall prohibit processing operation in case of non-compliance with the Directive.

3.4.4.4. SECTION 4 DATA PROTECTION OFFICER

Article 33 introduces a mandatory data protection officer of the controller who shall fulfil the tasks listed in Article 35. Where several competent authorities are acting under the supervision of a central authority, functioning as controller, at least this central authority should designate such 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 34 sets out the position of the data protection officer.

Article 35 provides the core tasks of the data protection officer.

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

Article 36 sets out the general principles for data transfers to third countries or international organisations, including onward transfers. It clarifies that transfers may take place to third countries in relation to which the Commission has adopted an adequacy decision or, in the absence of such decision, where appropriate safeguards are in placein a legally binding instrument, such as an international agreement.

Article 37 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 explicitly confirms 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 exclusively for the purposes of this Directive and in particular Article 36 paragraph 1.

Article 38 spells out and clarifies the derogations for data transfer, based on Article 26 of Directive 95/46/EC and Article 13 of Framework Decision 2008/977/JHA. Processing carried under these circumstances must have a legal basis in Union law, or the law of the Member State to which the controller is subject and which meets an objective of public interest or the need to protect the rights and freedoms of others, respects the essence of the right to the protection of personal data and is proportionate to the legitimate aim pursued.

Article 39 obliges Member States do ensure that processing restrictions are met by recipients of the personal data in the third country or international organisation. .

Article 40 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 Privacyof 12 June 2007.

Article 41 requires the Commission to report specifically on international transfers.

3.4.6. CHAPTER VI - NATIONAL SUPERVISORY AUTHORITIES

3.4.6.1. SECTION 1 INDEPENDENT STATUS

Article 42 obliges Member States to establish supervisory authorities, following Article 28(1) of Directive 95/46/EC, 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 43 clarifies the conditions for the independence of supervisory authorities, implementing case law by the Court of Justice[33], inspired also by Article 44 of Regulation

[33] European Court of Justice, judgment of 9.3.2010, Commission / Germany (C-518/07, ECR 2010 p. I-1885)

(EC) No 45/2001[34]. .Article 44 provides general conditions for the members of the supervisory authority, implementing the relevant case law[35], inspired also by Article 42(2)-(6) of Regulation (EC) 45/2001.

Article 45 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 46 on professional secrecy of the members and staff of the supervisory authority follows Article 28(7) of Directive 95/46/EC.

3.4.6.2. SECTION 2 DUTIES AND POWERS

Article 47 sets out the competence of the supervisory authorities, based on Article 28(6) of Directive 95/46/EC. 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 48 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 to access on behalf of data subjects and to check the lawfulness of the data processing.

Article 49 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, and Article 47 of Regulation (EC) 45/2001.

Article 50 obliges the supervisory authorities to draw up annual activity reports, based on Article 28(5) of Directive 95/46/EC.

3.4.7. CHAPTER VII – CO-OPERATION

Article 51 introduces explicit rules on mandatory mutual assistance, including consequences for non-compliance with the request of another supervisory, whereas Article 28 (6)2 of Directive 95/46/EC provided simply a general obligation to cooperate, without specifying it.

Article 52 introduces rules on joint operations, inspired by Article 17 of Council Decision 2008/615/JHA[36], including the possibility of supervisory authorities to participate in such operations.

Article 53 provides that the European Data Protection Advisory Board, established by the General Data Protection Regulation, exercises its tasks in relation to processing activities within the scope of this Directive.

---

34 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.

35 op. cit, footnote 33..

36 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1.

3.4.8. CHAPTER VIII - REMEDIES, LIABILITY AND SANCTIONS

Article 54 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 or, but only in case of a personal data breach, on its own behalf.

Article 55 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. Regarding the competence of the court, it provides that the proceedings can be brought either before the court of the supervisory authorities' Member State or before the court of the Member State where the data subject resides.

Article 56 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, and provides for the choice of the plaintiff to go to court in the Member State where the defendant is established or where the data subject resides.

Article 57 introduces common rules for court proceedings, including the rights of bodies, organisations or associations to represent data subjects before the courts, the right of supervisory authorities to engage in legal proceedings and, inspired by Article 5(1) of Framework Decision 2009/948/JHA[37] and by Article 13(1) of Council Regulation 1/2003[38], the information of the courts on parallel proceedings in another Member State, and the possibility for the courts to suspend the proceedings in such a case. The obligation of Member States to ensure rapid court actions (paragraph 10), is inspired by Article 18(1) of the eCommerce Directive 2000/31/EC[39].Article 58 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 59 obliges Member States to lay down rules on penalties, to sanction infringements of the Directive, and to ensure their implementation, including against the controller's representative.

3.4.9. CHAPTER IX – FURTHER SPECIFIC PROVISIONS

Article 60 concerns the transmission of personal data to authorities or private parties in the Union, inspired by Article 14 of Framework Decision 2008/977/JHA, and provides that such transmission is prohibited unless one of the exceptions set out in this Article applies. .

---

37 Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L 328 , 15/12/2009, p. 42.

38 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, p.1.

39 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.

3.4.10. CHAPTER X – DELEGATED ACTS AND IMPLEMENTING ACTS

Article 61 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 62 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.

3.4.11. CHAPTER XI – FINAL PROVISIONS

Article 63 repeals Framework Decision 2008/977/JHA.

Article 64 sets out that specific provisions in 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 65 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 with the Directive.

Article 66 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 67 determines the date of the entry into force of the Directive.

<EMPTY>/ (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

("Police and Criminal Justice Data Protection Directive")

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[40],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a 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 sharing and collection has increased spectacularly. Technology allows competent authorities to make use of personal data

[40] OJ C , , p. .

on an unprecedented scale in order to pursue their activities. 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 the protection of personal data.

(4) 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[41] 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 police and judicial cooperation in criminal matters.

(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 cooperation in criminal matters[42] applies in the areas of police and judicial cooperation in criminal matters. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) In order to ensure a consistent and high level of protection of the personal data of individuals and to remove the obstacles to disclosure of personal data to competent authorities of other Members States to ensure police and judicial cooperation in criminal matters, 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. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders 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 …../2011 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

---

41 OJ L 281, 23.11.1995, p. 31.

42 OJ L 350, 30.12.2008, p. 60.

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 cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation 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 specific 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 exchanges of data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of police and criminal justice.

(13) The protection afforded by this Directive should concern natural persons, whatever their nationality or place residence, in relation to the processing of personal data. It should not affect legislation on the protection of legal persons with regard to the processing of personal data concerning them.

(14) 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.

(15) 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.

(16) Given the importance of the developments under way in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate location data relating to natural persons, which may be used for different purposes including surveillance or creating profiles, this Directive should be applicable to processing involving such personal data.

(17) Any processing of personal data must be lawful, fair and transparent in relation towards the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the

collection of the personal data. The personal data should be adequate, relevant and limited to the minimum necessary for the purposes for which the personal data are processed; this requires in particular limiting the data collected and the period for which the data are stored to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate should be rectified or deleted. In order to ensure that the data are kept no longer than necessary, time limits should be established by the controller for erasure or periodic review.

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

(19) 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. .

(20) In order to be lawful, the processing of personal data should be necessary for the performance of a task carried out in the public interest by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in order to protect the vital interests of the data subject.

(21) Where processing is carried out for the performance of a task carried out in the public interest by a competent authority, it should be in compliance with a legal basis in Union law or Member State law which should contain explicit and detailed provisions at least as to the objectives, the personal data, the specific purposes and means, designate or allow to designate the controller, the procedures to be followed, the use and limitations of the scope of any discretion conferred to the competent authorities in relation to the processing activities.

(22) Competent authorities should only have access to personal data processed for purposes, other than those of this Directive, if authorised by law and if there are reasonable grounds that access will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and subject to appropriate safeguards.

(23) Any restriction of the data subject's rights must be in compliance with the Charter of Fundamental Rights of the European Union and with the Convention for the Protection of Human Rights and Freedoms, as clarified by the case law of the European Court of Justice and the European Court of Human Rights, and in particular respect the essence of the rights and freedoms.

(24) The processing of personal data for other purposes should be only allowed where the processing is compatible with the purposes for which the data have been initially collected. In case that the other purpose is not compatible with the initial one for

which the data are collected, the controller should base this processing of a legitimate ground for lawful processing. In any case, also as regards this further purpose, in particular the application of the principles set out by this Directive and in particular the information of the data subject on those other purposes should be ensured.

(25) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless processing is necessary for the performance of a task carried out in the public interest, on the basis of Union or Member State law which provide 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.

(26) The processing of genetic data should only be allowed if there is a genetic link which appears in the course of a criminal investigation or a judicial procedure. Genetic data should only be stored as long as strictly necessary for the purpose of such investigations and procedures, while Member States can provide for longer storage under the conditions set out in this Directive.

(27) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. Such measures which produce a legal effect for the data subject or significantly affects them should be prohibited, unless authorised by a law. In any case, such measure should be subject which should be safeguard to suitable measures to safeguard the data subject’s legitimate interests.

(28) The principle of transparency requires that any information of the data subject is easily accessible and easy to understand, and that clear and plain language is used.

(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 within a fixed deadline.

(30) The principles of fair and transparent processing require 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 he is obliged to provide the data and of the consequences, in cases he does 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 collected or otherwise processed.

(32) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. In this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

(33) 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 and verify the lawfulness of the processing. Every data subject should therefore the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing.

(34) Member States should be allowed to adopt legislative measures restricting or delaying the information of data subjects or the access to their 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. The controller should assess by way of concrete and individual examination if partial or complete restriction of the right of access should apply. 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 the competent national supervisory authority to exercise the right of access on their behalf. 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 a check has taken place, 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 personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the provisions adopted pursuant to this Directive. Where the personal data are contained in a judicial decision or record related to the issuance of a judicial decision, the rectification, erasure or 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 and be obliged to be able to demonstrate the compliance of each processing operation 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 require that appropriate technical and organisational measures be taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of the Directive are met. In order to ensure and demonstrate 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, also in relation to the monitoring and measures by the supervisory authorities, 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. The data subject should have the right to exercise his or her rights under this Directive in respect of and against each of the joint controllers.

(40) Processing activities should be documented by the controller or processor, in order to demonstrate 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 those processing operations.

(41) Every processing operation of personal data should be recorded in order to enable the verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.

(42) In order to maintain security and to prevent processing in breach of this Directive, the controller or processor should evaluate the risks inherent to the processing and implement measures to ensure a level of security appropriate to those risks, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected.

(43) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or 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 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. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned.

(44) 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 identity fraud or other forms 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.

(45) In order to ensure effective protection of the rights and freedoms of data subjects, procedures and mechanisms focussing on processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

(46) A data protection impact assessment should be carried out by the controller or processors, which should include in particular the envisaged measures, safeguards and mechanisms to ensure the protection of personal data and for demonstrating compliance with this Directive. Impact assessments should concern relevant systems and processes of a personal data processing operations, but not individual cases.

(47) Where a data protection impact assessment indicates that processing operations are likely to present a high degree of specific risks to the rights and freedoms of data subjects, the supervisory authority should be in a position to prevent, prior to the start of operations, a risky processing which is not in compliance with this Directive, and to make proposals to remedy such situation. Such consultation may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

(48) The controller or the processor should designate a person that would assist the controller or processor to monitor and demonstrate compliance with the provisions adopted pursuant to this Directive. Where several competent authorities are acting under the supervision of a central authority, at least this central authority should designate such data protection officer. The data protection officers must be in a position to perform their duties and tasks independently.

(49) Member States should ensure that a transfer to a third country may only take place if the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or where appropriate safeguards have been adduced by way of a legally binding instrument. The transfer of data should only take 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.

(50) The Commission may recognise that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of protection, thus providing an added value of legal certainty and uniformity throughout the Union. In these cases, transfers of personal data may take place to these countries without needing to fulfil any specific formal requirement.

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

(52) The Commission should equally be able to recognise that a third country offers no adequate level of protection; consequently the transfer of personal data to that third country should be prohibited; provision should be made for procedures for negotiations between the Commission and such third countries.

(53) Transfers which are not based on such 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.

(54) 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, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their foreign counterparts.

(55) 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.

(56) Member States may entrust 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.

(57) 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 the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union.

(58) 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.

(59) 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 and to ensure the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(60) 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 strictly limited to genuine judicial activities in court cases and not apply for other activities where judges might be involved in accordance with national law.

(61) 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.

(62) 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.

(63) 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. Each supervisory authority should be ready to participate in joint operations. The requested supervisory authority should be obliged to respond in a defined time period to the request.

(64) 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 react on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(65) 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, or to lodge a complaint on its own behalf where it considers that a personal data breach has occurred.

(66) 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 may be brought either before the courts of the Member State where the supervisory authority is established or before the courts of the Member State where the data subject has his or her habitual residence. For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides.

(67) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. 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.

(68) 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 establishes fault on the part of the data subject or in case of force majeure.

(69) Penalties should be imposed on any 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.

(70) Regulation (EU)…./2012 establishes a European Data Protection Board. The Commission should participate in its activities. The European Data Protection Board should also contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(71) Transmission of personal data to other authorities or private parties in the Union is prohibited unless the transmission is in compliance with law, and the recipient is established in a Member State, and no legitimate specific interests of the data subject prevent transmission, and the transmission is necessary in a specific case for the controller transmitting the data for either the performance of a task lawfully assigned to it, or the prevention of an immediate and serious danger to public security, or the prevention of serious harm to the rights of individuals. The controller should inform the recipient of the purpose of the processing and the supervisory authority of the transmission. The recipient should also be informed of processing restrictions and ensure that they are met.

(72) 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 procedures and mechanisms for exercising the rights of the data subject, information to the data subject, the right of access, the right to erasure, responsibility of the controller, data protection by design and by default, the processor, documentation, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation, designation and tasks of the data protection officer. 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.

(73) In order to ensure uniform conditions for the implementation of this Directive of the procedures for access by competent authorities, modalities for exercising the rights of data subjects, information to the data subject, the right of access, data protection by design and by default, documentation, security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation, 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 and mutual assistance, 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[43].

(74) The examination procedure should be used for the adoption of the procedures for access by competent authorities, modalities for exercising the rights of data subjects, information to the data subject, the right of access, data protection by design and by default, documentation, security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation, 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 and mutual assistance, , given that those acts are of general scope.

(75) 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 and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.

(76) 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 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

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

(78) Specific provisions in acts concerning police co-operation and judicial co-operation in criminal matters which are 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 specific provisions with the Directive.

(79) 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

---

[43] 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 Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.

this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

(80) 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.

(81) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[44].

(82) 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[45].

(83) 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[46].

(84) 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.

---

44 OJ L 176, 10.7.1999, p. 36.
45 OJ L 53, 27.2.2008, p. 52
46 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 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, erasure or destruction;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) '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;

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

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

(8) '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;

(9) 'genetic data' means all data, of whatever type, concerning the hereditary characteristics of an individual;

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

(11) ‘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, and which may include: 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; and identification of a person (healthcare professional) as provider of healthcare to the individual;

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

(13) 'competent authorities' means any public authority competent for the prevention, detection and investigation of criminal offences, authorised by law to process personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(14) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 42.

CHAPTER II
PRINCIPLES

Article 4
Principles relating to personal data processing

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

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) collected for specified, explicit and legitimate purposes and may only be further processed for another compatible purpose in accordance with Article 8;

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed and shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not make it possible or no longer makes it possible to identify the data subject;

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

(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 and demonstrate, for each processing operation, compliance with the provisions adopted pursuant to this Directive;

(g) accessed by or made available only to those duly authorised staff in competent authorities who need them for the performance of their tasks.

2. Member States shall provide that competent authorities may only have access to personal data initially processed for purposes other than those referred to in Article 1(1), are specifically authorised by law which must meet the requirements set out in paragraph 3 and must provide that:

(a) access is allowed only by duly authorised staff of the competent authorities in the performance of their tasks where, in a specific case, reasonable grounds give reason to to consider that the processing of the personal data will

substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) requests for access must be in writing and refer to the legal ground for the request; and

(c) appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data. Member States may subject the access to the personal data to additional conditions such as judicial authorisation, in accordance with their national law.

3. Union or Member State law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions at least as to:

(a) the objectives to be pursued by the processing;

(b) the personal data to be processed;

(c) the specific purposes and means of processing;

(d) the designation of the controller, or of the specific criteria for the nominationof the controller;

(e) the categories of duly authorised staff of the competent authorities for the processing of the personal data data,

(f) the procedure to be followed for the processing;

(g) the use that may be made of the personal data obtained;

(h) limitations to the scope of any discretion conferred to the competent authorities in relation to the processing activities.

4. Member States shall provide that any personal data processed in breach of the provisions adopted pursuant to this Directive shall no longer be processed.

5. The Commission may specify procedures for access to information referred to in paragraph 2, in particular as regards the format for the request and standards for handover of the data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 5

Distinction between different categories of data subjects

1. Member States shall ensure that the controller makes a clear distinction between personal data of

(a) persons where 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.

2. Member States shall provide for specific guarantees for the processing of personal data relating to persons who are not convicted of a criminal offence, or where in relation to them are no serious grounds for believing that they have committed a criminal offence.

Article 6

Different degrees of accuracy and reliability of personal data

1. Member States shall ensure that 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 personal data based on facts is distinguished from personal data based on personal assessments.

Article 7

Lawfulness of processing

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

(a) processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1); or

(b) processing is necessary in order to protect the vital interests of the data subject.

2. Processing based on point (a) of paragraph 1 must be provided for in:

(a) Union law; or

(b) the law of the Member State to which the controller is subject; this law must meet an objective of public interest and the requirements referred to in Article 4(3).

Article 8

Change of purpose of the processing

1. Member States shall provide that personal data may only be further processed for another purpose which is compatible with the purposes for which the data were collected.

2. Where another purpose is not compatible with that for which the personal data are collected, the processing must have a legal basis in point (a) or (b) of Article 7(1).

Article 9

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, and the processing of genetic data or data concerning health or sex life.

2. Paragraph 1 shall not apply where:

   (a) the processing is necessary for the performance of a task carried out in the public interest, on the basis of Union or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests, including specific authorisation from a judicial authority, if required by Member State's law;

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

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

Article 10

Processing of genetic data for the purpose of a criminal investigation or a judicial procedure

1. Member States shall ensure that genetic data may only be used to establish a genetic link in the framework of adducing evidence, preventing a threat to public security or suppressing a specific criminal offence. Genetic data may not be used to determine other characteristics which may be linked genetically.

2. Member States shall provide that genetic data or information derived from their analysis may only be retained where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to strict storage periods to be determined by national law.

3. Member States shall ensure that genetic data or information derived from their analysis is only stored for longer periods when the genetic data cannot be attributed to an individual, in particular when it is found at the scene of a crime.

Article 11

Measures based on profiling

1. Member States shall provide that measures which produces a legal effect for the data subject or significantly affects them and which are based on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless they 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 exclusively on special categories of personal data referred to in Article 9.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 12

Modalities for exercising the rights of the data subject

1. Member States shall provide that the controller has 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, adapted to the data subject, in particular for any information addressed specifically to a child.

3. Member States shall provide that the controller establishes procedures for providing the information referred to in Article 13 and for the exercise of the rights of data subjects referred to in Articles 14 to 19. Where personal data are processed by automated means, the controller shall provide also means for requests to be made electronically.

4. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Articles 14 to 19. That information shall be given in writing. Where the data subject makes the request in electronic form, the information may be provided in electronic form. As regards the right of access

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

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and conditions for manifestly excessive requests and the fees referred to in paragraph 5.

7. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 13
Information to the data subject

1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller provides 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 or erasure of the personal data concerning the data subject;

   (e) the right to lodge a complaint to the supervisory authority referred to in Article 42 and its contact details;

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

   (g) where applicable, that the controller intends to transfer to a third country or international organisation, on the level of protection afforded by that third country or international organisation, and on potential access to the data transferred by authorities to that third country or international organisation under the rules of that third country or international organisation;

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

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, on 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 collected or otherwise processed.

4. Member States may adopt legislative measures restricting or delaying the application of paragraphs 1 and 2 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 shall provide that the controller assesses, in each specific case, by way of a concrete and individual examination whether a partial or complete restriction for one the reasons referred to in paragraph 4 applies. Member States may also determine categories of data processing which may wholly or partly fall under the exemptions under points (a), (b), (c) and (d) of paragraph 4.

6. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 4, taking into account the specific characteristics and needs of various data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 14
Right of access for the data subject

1. Member States shall provide for the right of the data subject to obtain from the controller at any time 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 are to be or have been disclosed, in particular to 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 or erasure of personal data concerning the data subject;

(f) the right to lodge a complaint to the supervisory authority and to provide the contact details of the supervisory authority;

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

(h) the significance and envisaged consequences of such processing at least in the case of measures referred to in Article 11.

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.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 15
Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that 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.

2. Member States shall provide that the controller assesses, in each specific, case by way of a concrete and individual examination whether a partial or complete restriction for one of the reasons referred to in paragraph 1 applies. Member States may also determine categories of data processing which may wholly or partly fall under the exemptions under points (a) to (d) of paragraph 1.

3. Member States shall provide that the controller shall inform 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 a reason under paragraph 1 exists.

4. Member States shall ensure that the controller documents the assessment referred to in paragraph 2 as well as the grounds for omitting the communication of the factual or legal reasons on which the decision is based.

Article 16
Modalities for exercising the right of access

1. Member States shall provide for the right of the data subject to request in cases referred to in Article 15, at all times, the supervisory authority to exercise the right of access on their behalf, and to check the lawfulness of the processing.

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

3. When access is exercised by the supervisory authority on behalf of the data subject, the supervisory authority shall inform the data subject at least that a check has taken place, 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 17
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 when their processing does not comply with the provisions adopted pursuant to this Directive. This shall be the case in particular because of the incomplete and inaccurate nature of these personal data. 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 18
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 this Directive.

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

3. Instead of erasure, the controller shall restrict processing of 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 controller no longer needs them for the accomplishment of its task but they have to be maintained for purposes of proof;

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

4. Personal data referred to in paragraph 3 may only be processed for purposes of proof or for the protection of public interest.

5. Where processing of personal data is restricted pursuant to paragraph 3, the controller shall inform the data subject before lifting the restriction on processing.

6. Member States shall provide that controller puts mechanisms in place to ensure that the time limits established for the erasure of personal data and for a periodic review of the need for the storage of the data are observed.

7. Where the erasure is carried out, the controller shall not otherwise process such personal data.

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

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and conditions as regards personal data identified for the purpose of restricting its processing as referred to in paragraph 3.

Article 19

Rectification, erasure and restriction of processing in judicial proceedings

Member States shall provide that the rectification, erasure or restriction of processing is carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record related to the issuance of a judicial decision.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 20
Responsibility of the controller

1. Member States shall provide that the controller adopts policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive, including the assignment of responsibilities, and the training of staff involved in the processing operations.

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

   (a) keeping the documentation referred to in Article 25;

   (b) implementing the data security requirements laid down in Article 28;

   (c) performing a data protection impact assessment pursuant to Article 31;

   (d) complying with the requirements for prior consultation pursuant to Article 32;

   (e) designating a data protection officer pursuant to Article 33.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. This verification shall be carried out by independent internal or external auditors, if proportionate.

4. Wherever the controller publishes or is required by law to publish a regular report of its activities, such report shall contain the controller's policies in relation to the protection of personal data, the risks linked to the data processing by the controller and the measure taken to mitigate such risks, unless such publication is likely to jeopardize the protection of public interests or the security of processing .

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, and the conditions for the verification mechanisms referred to in paragraph 4.

Article 21

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 both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of 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 are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements across products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 22

Joint controllers

1. 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 obligations under this Directive by means of an arrangement between them. If the arrangement between the joint controllers does not determine the respective responsibilities in relation to those obligations, the responsibility of those joint controllers to comply with the provision adopted pursuant to this Directive shall be solidary.

2. The data subject may exercise their rights under this Directive in respect of and against each of the joint controllers.

Article 23

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 in particular in respect of the technical security measures and

organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. Member States shall provide that the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller; in particular, where the transfer of the personal data used is prohibited unless the processor is so instructed by the controller;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 28;

(d) enlist another processor only with the permission of the controller and therefore inform the controller of the intention to enlist another processor in such a timely fashion that the controller has the possibility to object;

(e) insofar as this is possible given the nature of the processing, adopt in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 28 to 32.

(g) hand all results over to the controller after the end of the processing and not process the personal data otherwise;

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 22.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1.

Article 24

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 25
Documentation

1. Member States shall provide that each controller and processor maintains documentation of all processing operations 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 name and contact details of the data protection officer;

   (c) the purposes of the processing;

   (d) an indication of the parts of the controller's or processor's organisation entrusted with the processing of personal data for a particular purpose;

   (e) a description of the category or categories of data subjects and of the data or categories of data relating to them;

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

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

   (h) a general indication of the time limits for erasure of the different categories of data;

   (i) the results of the verifications of the measures referred to in Article 20(1);

   (j) an indication of the legal basis of the processing operation for which the data are intended.

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

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor.

5. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 26
Keeping of records

1. Member States shall ensure that all processing operations of personal data are recorded for the purposes of verification of the lawfulness of the data processing.

These records shall show in particular the purpose of the access, the data and time of access and the recipients of personal data.

2. Records referred to in paragraph 1 shall be notified on request to the competent supervisory authority. The competent supervisory authority shall use this information only for the monitoring of compliance with the provisions adopted pursuant to this Directive.

3. The records shall not be used for any other purposes, except for the purposes of self-monitoring and for ensuring data integrity and security.

Article 27
Cooperation with the supervisory authority

1. Member States shall provide that the controller and the processor shall cooperate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 49(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under point (b) of Article 49(1), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

SECTION 2
DATA SECURITY

Article 28
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. Member States shall provide that processors may be designated only if they guarantee that they observe the requisite technical and organisational measures under paragraph 1 and comply with the instructions under Article 23(2)(a). The competent authority shall monitor the processor in those respects.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 to 3 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 29

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, as a rule, not later than 24 hours after the personal data breach has been established, the personal data breach to the supervisory authority.

2. Pursuant to point (f) of Article 23(2) the processor shall alert and inform the controller immediately after the detection 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 concerned;

   (b) communicate the identity and contact details of the data protection officer referred to in Article 33 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 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 61 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 62(2).

Article 30

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 communicates, in addition to the notification referred to in Article 29, the personal data breach to the data subject without undue delay and, as a rule, not later than 24 hours after the personal data breach has been established by the controller.

2. The communication to the data subject may be delayed or omitted in accordance with Article 13(4).

3. The communication to the data subject referred to in paragraph 1 shall contain the information and the recommendations provided for in points (a) to (c) of Article 29(3).

4. The communication of a personal data breach to the data subject shall not be required if the controller has demonstrated 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.

5. Without prejudice to the controller's obligation to notify the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

7. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 31
Data protection impact assessment

1. Member States shall provide that, prior to the processing of personal data, the controller or the processor carries out an assessment of the impact of the envisaged processing systems and procedures on the protection of personal data, where the processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

2. In particular the following processing operations are likely to present such specific risks as referred to in paragraph 1:

   (a) processing of personal data in large scale filing systems for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties;

   (b) processing of special categories of personal data under the meaning of Article 9, of personal data related to children and of biometric data for the purposes of

the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties.

(c) an evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's behaviour, which is based on automated processing and likely to result in measures that produces legal effects concerning the individual or significantly affects the individual; or

(d) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance); or

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to Article 32(1).

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

4. Member States shall provide that the controller consults the public on the intended processing, without prejudice to the protection of public interests or the security of the processing operations.

5. Without prejudice to the protection of public interests or the security of the processing operations, the assessment shall be made easily accessible to the public.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 32

Prior consultation of the supervisory authority

1. Member States shall provide that the controller or the processor consults the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with the provisions adopted pursuant to this Directive and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 31 indicates that processing operations by virtue of their nature, their scope and/or their purposes, are likely to present a high degree of specific risks; or

(b) the supervisory authority deems it necessary to carry out a prior consultation on specified processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

2. Where the supervisory authority is of the opinion that the intended processing does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

3. The supervisory authority shall establish a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate that list to the controllers and to the European Data Protection Board.

4. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for to in Article 31 and, on request, with any other information to allow the supervisory authority to make an assessment on the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

5. If the supervisory authority is of the opinion that the intended processing does not comply with the provisions adopted pursuant to this Directive or that risks are insufficiently identified or mitigated, it shall make appropriate proposals to remedy such incompliance.

6. Member States may consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing under this Directive, and in particular to mitigate the risks involved for the data subjects.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (b) of paragraph 1.

8. The Commission may set out standard forms and procedures for prior consultations referred to in paragraphs 1, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

SECTION 4

DATA PROTECTION OFFICER

Article 33

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 35. The necessary level of expert knowledge shall be determined in particular by the data processing carried out and the protection required by the personal data processed by the controller or the processor.

3. Member States shall provide that controller or the processor ensures that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

4. The data protection officer shall be designated for a period of at least two years. The data protection officer may be reappointed for further terms. During the term of office, the data protection officer may only be dismissed from that function, if they no longer fulfil the conditions required for the performance of their duties.

5. Member States shall provide that the controller or the processor communicates the name and contact details of the data protection officer to the supervisory authority and to the data subject pursuant to Article 13(1)(a).

6. Member States shall provide for the data subject the right to contact the data protection officer on all issues related to the processing of their personal data.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements for the criteria for the professional qualities of the data protection officer referred to in paragraph 1.

Article 34
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 performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks as referred to in Article 35.

Article 35
Tasks of the data protection officer

1. 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 this Directive;

(d) to ensure that the documentation referred to in Article 25 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 29 and 30;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior consultation, if required pursuant to Articles 31 and 32;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating 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.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 61 for the purpose of specifying further the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 36

General principles for transfers of personal data

1. 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, may take place only if:

(a) the level of protection of individuals for the protection of personal data guaranteed in the Union by this Directive is not undermined;

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

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

(d) the conditions laid down in paragraph 2 and in Articles 37 to 39 are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation; and

(e) the other provisions adopted pursuant of this Directive are complied with by the controller and processor.

2. Member States shall provide that a transfer, subject to the conditions set out in paragraph 1, may only take place:

(a) where the Commission has decided under the conditions and procedure referred to in Article 37 that the third country or international organisation in question ensures an adequate level of protection; or

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

Article 37
Transfers with an adequacy decision

1. Member States shall provide that a transfer may only take place where the Commission has decided in accordance with Article 38 of Regulation (EU) …./2012 or in accordance with paragraph 3 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 authorization.

2. The adequacy of the level of protection shall be assessed by the Commission, taking into account:

(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 Union data subjects whose personal data are being transferred;

(b) the existence and effective functioning of an independent supervisory authority 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 his or her 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 62(2).

4. The implementing act shall specify its geographical and sectoral application, and 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 62(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 62(3).

6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5.

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 38
Derogations

1. In the absence of an adequacy decision pursuant to Article 37 or of appropriate safeguards pursuant to Article 36(2)(b), Member States shall provide that , a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the transfer is necessary for grounds of public interest; or

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

(c) the transfer is necessary to safeguard law legitimate interests of the data subject where the law of the Member State transferring the data provides so; or

(d) 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.

2. Processing based on paragraph 1 must have a legal basis in Union law, or the law of the Member State to which the controller is subject; this law must meet an objective of public interest or the need to protect the rights and freedoms of others, respects the essence of the right to the protection of personal data and is proportionate to the legitimate aim pursued.

Article 39
Specific conditions for the transfer of data

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

Article 40
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 37(3).

Article 41
Report by the Commission

The Commission shall submit a report on the application of Articles 36 to 40 to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Directive. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall supply this information without undue delay. The report shall be made public.

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 42
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 cooperate with each other and the Commission.

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

Article 43
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 States shall provide that the members of the supervisory authority l, 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 the duties of the office and shall not, during their term of office, engage in any other 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 be subject to the direction of the head of the supervisory authority.

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

Article 44

General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority are to be appointed either by the parliament or the government of the Member State concerned and that the general conditions set out in paragraphs 2 to 5 are to be complied with.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.

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 to 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 is guilty of serious misconduct.

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

Article 45

Rules on the establishment of the supervisory authority

Each Member State shall provide by law:

(a) the establishment and status of the supervisory authority;

(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 in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Article 46
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 47
Competence

1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.

2. The supervisory authority shall not be competent to supervise processing operations of courts when acting in their judicial capacity.

Article 48
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 that data subject in accordance with Article 54, investigates, to the extent appropriate, the matter and informs the data subject or 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) to exercise the right of access on behalf of a data subject and check the lawfulness of data processing pursuant to Article 16, 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 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 inquiries 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 32;

(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 under this Directive, and, if appropriate, cooperate 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 obviously excessive, in particular by their repetitive character, the supervisory authority may charge a fee or not take the action required by the data subject. In such case, the supervisory authority shall bear the burden of proving of the excessive character of the request.

Article 49
Powers

1. Member States shall provide that each supervisory authority has the power:

(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;

(b) to order the controller to comply with the data subject's requests to exercise the rights under this Directive, including those provided by Articles 14 to 19 where such requests have been refused in breach of those provisions;

(c) to order the controller or the processor to provide the information pursuant to Article 12(1) and (2) and Articles 13, 29 and 30;

(d) to ensure the compliance with opinions on prior consultations referred to in Article 32;

(e) to warn or admonish the controller or the processor;

(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions adopted pursuant to this Directive and the notification of such actions to third parties to whom the data have been disclosed;

(g) to impose a temporary or definitive ban on processing;

(h) to suspend data flows to a recipient in a third country or to an international organisation;

(i) to inform national parliaments, the government or other political institutions as well as the public on the matter.

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

(a) access to all personal data and to all information necessary for the performance of its supervisory,

(b) access to any of its premises, including to any data processing equipment and means, in accordance with national law, where there are reasonable grounds for presuming that an activity in violation of the provisions adopted pursuant to this Directive is being carried out there, without prejudice to a judicial authorisation if required by national law.

3. Each supervisory authority shall have the power to bring violations of the provisions adopted pursuant to this Directive to the attention of the judicial authorities and to engage in legal proceedings and bring an action to the competent court pursuant to Article 57(2).

4. Each supervisory authority shall have the power to sanction administrative offences.

Article 50
Activities report

Member States shall provide that each supervisory authority draws up an annual report on its activities. The report shall be presented to the national parliament and shall be made available to the public, the Commission and the European Data Protection Board.

CHAPTER VII
CO-OPERATION

Article 51
Mutual assistance

1. Member States shall provide that supervisory authorities provide each other mutual assistance in order to implement and apply the provisions pursuant this Directive in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.

2. Member States shall provide that each supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority. Such measures may include, in particular, enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Directive without delay and not later than one month after having received the request.

3. The request for assistance shall contain all the necessary information, including the purpose of the request, and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.

4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

   (a) it is not competent for the request; or

   (b) compliance with the request would be incompatible with the provisions adopted pursuant to this Directive.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.

6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.

7. No fee shall be charged for any action taken following a request for mutual assistance.

8. The Commission may specify the format and procedures for mutual assistance referred to in this article; the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 52
Joint operations

1. Member States shall provide that, in order to step up cooperation and mutual assistance, the supervisory authorities may carry out joint enforcement measures and other joint operations in which designated members or staff from supervisory authorities of other Member States participate in operations within a Member State's territory.

2. Member States shall provide that in cases where data subjects in another Member State or other Member States are likely to be affected by processing operations, the competent supervisory authority may be invited to participate in the joint operations. The competent supervisory authority may invite the supervisory authority of each of those Member States to take part in the respective operation and in case where it is invited, respond to the request of a supervisory authority to participate in the operations without delay.

3. Each Member State may, as a host Member State, in compliance with its own national law, and with the seconding Member State's authorization, confer executive powers on the members or staff of the supervisory authority of the seconding Member State involved in joint operations or, in so far as the host Member State's law permits, allow the members or staff of the supervisory authority of the seconding Member State to exercise their executive powers in accordance with the seconding Member State's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the supervisory authority of the host Member State. The seconding Member States' officers shall be subject to the host Member State's national law. The host Member State shall assume responsibility for their actions.

4. Member States shall lay down the practical aspects of specific co-operation actions.

Article 53
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 cooperation 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 62 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 54

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.

3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2 to lodge a complaint with a supervisory authority in any Member State also on its own behalf if it considers that Articles 29 or 30 have been infringed as a result of the processing of its personal data.

Article 55

Right to a judicial remedy against a supervisory authority

1. Member States shall provide for the right for each natural or legal person to a judicial remedy against decisions of a supervisory authority concerning them.

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 Article 48(1)(b).

3. Proceedings against a supervisory authority may be brought either before the courts of the Member State where the supervisory authority is established or before the courts of the Member State where the data subject has the habitual residence.

4. Member States shall undertake mutually to enforce final decisions handed down by the courts referred to in this Article.

Article 56

Right to a judicial remedy against a controller or processor

1. 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 person to a judicial remedy if they consider that that his or her rights under this Directive have been infringed as a result of the processing of their personal data in non-compliance with the provisions adopted pursuant to this Directive.

2. Proceedings against a controller or a processor may be brought either before the courts of the Member State where the controller is established or before the courts of the Member State where the data subject has the habitual residence.

3. Member States shall undertake mutually to enforce final decisions handed down by the courts referred to in this Article.

Article 57

Common rules for court proceedings

1. Member States shall provide for the right of any body, organisation or association referred to in Article 54(2) to exercise the rights referred to in Article 55 and 56 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 provide that, where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, that court contacts the competent court in the other Member State to confirm the existence of such parallel proceedings.

4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, Member States shall provide for the possibility of the court to suspend the proceedings.

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

Article 58

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 59

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
TRANSMISSION TO OTHER PARTIES

Article 60

Transmission to other authorities or private parties in the European Union

1. Member States shall ensure that the controller does not transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to this Directive, unless

   (a) the transmission is in compliance with European Union or Member State law; and

   (b) the receiving natural or legal person is established in a Member State of the European Union; and

   (c) no legitimate specific interests of the data subject prevent transmission; and

   (d) the transmission is necessary in a specific case for the controller transmitting the personal data for:

      (i) the performance of a task lawfully assigned to it; or

      (ii) the prevention of an immediate and serious danger to public security; or

      (iii) the prevention of serious harm to the rights of individuals.

2. The controller shall inform the recipient of the purpose for which the personal data may exclusively be processed.

3. The controller shall inform the supervisory authority of such transmissions.

4. The controller shall inform the recipient of processing restrictions and ensure that these restrictions are met.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 61

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 Articles 12(6), 13(6), 14(3), 18(9), 20(5), 21(3), 23(4), 25(4), 29(5), 30(6), 31(6), 32(7), 33(8) and 35(2) 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 12(6), 13(6), 14(3), 18(9), 20(5), 21(3), 23(4), 25(4), 29(5), 30(6), 31(6), 32(7), 33(8) and 35(2) 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 12(6), 13(6), 14(3), 18(9), 20(5), 21(3), 23(4), 25(4), 29(5), 30(6), 31(6), 32(7), 33(7) and 35(2) 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 62
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 XI
FINAL PROVISIONS

Article 63
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 64

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

The specific provisions for the protection of personal data in acts 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 65

Evaluation

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

2. The Commission shall review within *one year after the entry into force of this Directive* other Acts adopted by the European Union which regulate the protection and processing of personal data, in particular those acts adopted by the Union referred to in Article 64, 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 paragraphs 1 and 2 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 66

Implementation

1. Member States shall adopt and publish, by 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 .

   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 notify to the Commission the text of the provisions of national law which they adopt pursuant to this Directive, by the date specified in Article 67(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 67
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 68
Addressees

This Directive is addressed to the Member States.

Done at Brussels,

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