EUROPEAN COMMISSION

Brussels, XXX
[…](2011) XXX draft

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)

(Text with EEA relevance)

Version 56
(29/11/2011)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

This explanatory memorandum presents in further detail the Commission's approach to a new legal framework for the protection of personal data in the EU as set out in Communication COM (2012) xxx final[1]. The proposed new 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 this first legislative proposal for a General Data Protection Regulation.

The centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC[2], 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 Framework Decision 2008/977/JHA as a general instrument at Union level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters[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

---

1 (insert title)

2 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, 23.11.1995, p.31. ('Directive').

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. ('Framework Decision').

a central role in the Digital Agenda for Europe[4], and more generally in the Europe 2020 Strategy[5].

The Lisbon Treaty defines the right to personal data protection as a principle of the EU and introduced with Article 16 of the Treaty on the Functioning of the European Union (TFEU) a specific legal basis for the adoption of rules on the protection of personal data. 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[6]. In its resolution on the Stockholm Programme, the European Parliament[7] 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[8] 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"[9], 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 personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity[10]. 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.

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

This initiative is the result of extensive consultations with all major stakeholders on a review of the current legal framework for the protection of personal data, which lasted for more than two years and included a high level conference in May 2009[11] and two phases of public consultation:

---

4 COM(2010)245 final.

5 COM(2010)2020 final.

6 "The Stockholm Programme — An open and secure Europe serving and protecting citizens", OJ C115, 4.5.2010, p.1.

7 Resolution of the European Parliament on the on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme adopted 25 November 2009 (P7_TA(2009)0090).

8 COM(2010)171 final.

9 COM(2010)609 final.

10 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 .

11 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm.

– 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.[12]

– 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.[13]

Targeted consultations were also conducted with key stakeholders; specific events were organised in June and July 2010 with Member State authorities and with private sector stakeholders, as well as privacy, data protection and consumers' organisations[14]. In November 2010, European Commission's Vice-President Reding organised a roundtable on the data protection reform. On 28 January 2011 (Data Protection Day), the European Commission and the Council of Europe co-organised a high level conference to discuss issues related to the reform of the EU legal framework as well as to the need for common data protection standards worldwide[15]. Two conferences on data protection were hosted by the Hungarian and Polish Presidencies of the Council on 16-17 June 2011 and on 21 September 2011 respectively.

Dedicated workshops and seminars on specific issues were held throughout 2011. In January ENISA[16] organised a workshop on data breach notifications in Europe[17]. In February, the Commission convened a workshop with Member States' authorities to discuss data protection issues in the area of police co-operation and judicial co-operation in criminal matters, including the implementation of the Framework Decision, and the Fundamental Rights Agency held a stakeholder consultation meeting on "Data Protection and Privacy". A discussion on key issues of the reform was held on 13 July 2011 with national Data Protection Authorities. EU citizens were consulted through a Eurobarometer survey held in November-December 2010[18]. A number of studies were also launched.[19] The "Article 29 Working Party"[20] provided several opinions and useful input to the Commission[21]. The European Data

---

12 The non-confidential contributions can be consulted on the Commission's website: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

13 The non-confidential contributions can be consulted on the Commission's website: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

14 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.

15 http://www.data-protection-day.net/init.xhtml?event=36.

16 European Network and Information Security Agency, dealing with security issues related to communication networks and information systems.

17 See http://www.enisa.europa.eu/act/it/data-breach-notification/.

18 Op cit. footnote 9.

19 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)..

20 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.

21 See in particular the following opinions: on the "Future of Privacy" (2009, WP 168); on the concepts of "controller" and "processor" (1/2010, WP 169); on online behavioural advertising (2/2010, WP 171); on the principle of accountability (3/2010, WP 173); on applicable law (8/2010, WP 179); and on consent

Protection Supervisor also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication[22].

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.[23] 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 many elements of the Commission's approach. The European Economic and Social Committee likewise 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.[24]

During the consultations on the comprehensive approach, a large majority of stakeholders agreed that the general principles remain valid but that there is a need to adapt the current framework in order to better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalisation, while maintaining the technological neutrality of the legal framework. Heavy criticism has been expressed regarding the current fragmentation of personal data protection in the Union, in particular by economic stakeholders who asked for increased legal certainty and harmonisation of the rules on the protection of personal data. The complexity of the rules on international transfers of personal data is considered as constituting a substantial impediment to their operations as they regularly need to transfer personal data from the EU to other parts of the world.

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 co-operation 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 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

---

(15/2011, WP 187). Upon the Commission's request, it adopted also the three following Advice Papers: on notifications, on sensitive data and on on the practical implementation of rticle 28(6) of the Data Protection Directive. They can all be accessed at: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

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

23 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).

24 CESE 999/2011.

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 delivered an opinion on the draft impact assessment on 9 September 2011. Following the IAB opinion, 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;

– A section on proportionality was added;

– All calculations and estimations related to administrative burden in the baseline scenario and in the preferred option have been entirely reviewed and revised, and the relation between the costs of notifications and the overall fragmentation costs has been clarified (including Annex 10);

– Impacts on small and medium enterprises, particularly of data protection officers and data protection impact assessments have been better specified.

The impact assessment report and an executive summary are published with the proposals.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal Basis

This proposal is based on Article 16 TFEU as the appropriate basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.

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 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, requires the same level of data protection throughout the Union. The absence of common EU rules would create the risk of different levels of protection in the Member States and create restrictions on cross-border flows of personal data between Member States with different standards.

– 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 co-operation 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 will 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.

3.3. Summary of fundamental rights issues

The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU and in Article 8 of the ECHR. As underlined by the Court of Justice of the EU[25], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[26]. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by 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 following: freedom of expression (Article 11 of the Charter); freedom to conduct a business (Article 16);

---

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

26 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.

the right to property and in particular the protection of intellectual property(Article 17(2)); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right to an effective remedy and a fair trial (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 Regulation, and, as in Article 1 of Directive 95/46/EC, the two objectives of the Regulation.

Article 2 determines the scope of the Regulation.

Article 3 contains the definitions for terms used in the Regulation. While some definitions are taken over from Directive 95/46/EC, others are modified, complemented with additional elements, or newly introduced ('personal data breach' based on Article 2(i) of the e-privacy Directive 2002/58/EC[27] as amended by Directive 2009/136/EC[28], 'genetic data', 'biometric data', 'data concerning health' which is based on the definition of 'health data' provided for by ISO 27799[29], 'main establishment', 'representative', 'enterprise', 'group of undertakings', 'binding corporate rules', and of a 'child' which is based on the United Nation's Convention on the Rights of the Child[30]).

In the definition of consent, the criterion 'explicit' is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.

3.4.2. CHAPTER II - PRINCIPLES

Article 4 sets out the principles relating to personal data processing, which correspond to those in Article 6 of Directive 95/46/EC. Additional new elements are in particular the transparency principle, the clarification of the data minimisation principle and the establishment of a comprehensive responsibility and liability of the controller.

Article 5 sets out, based on Article 7 of Directive 95/46/EC, the criteria for lawful processing, which are further specified as regards the balance of interest criterion and processing for the purposes of direct marketing for commercial purposes, the compliance with legal obligations and public interest.

---

27 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 , 31/07/2002, p. 37.

28 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance; OJ L 337 , 18.12.2009, p. 11.

29 ISO 27799:2008 'Health informatics — Information security management in health using ISO/IEC 27002'.

30 Adopted and opened for signature, ratification and accession by the United Nations General Assembly resolution 44/25 of 20.11.1989

Article 6 clarifies the conditions the change of purpose of the processing, i.e. for another purpose than that for which the data have been initially collected.

Article 7 clarifies the conditions for consent to be valid as a legal ground for lawful processing.

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

3.4.3. CHAPTER III - RIGHTS OF THE DATA SUBJECT

3.4.3.1. Section 1 – Transparency and modalities

Article 9 introduces the obligation for transparent and easily accessible and understandable information, inspired in particular by the Madrid Resolution on international standards on the protection of personal data and privacy[31].

Article 10 obliges the controller to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined a deadline, and the motivation of refusals.

Article 11 provides rights in relation to recipients, based on Article 12(c) of Directive 95/46/EC, extended to all recipients, including joint controllers and processors.

3.4.3.2. Section 2 – Information and access to data

Article 12 specifies the controller's information obligations towards the data subject, building on Articles 10 and 11 of Directive 95/46/EC, providing additional information to the data subject, including on the storage period, the right to lodge a complaint, in relation to international transfers and to the source from which the data are originating.

Article 13 provides the data subject's right of access to their personal data, building on Article 12(a) of Directive 95/46/EC and adding new elements, such as to inform the data subjects on the storage period, rights to rectification and erasure and to lodge a complaint.

3.4.3.3. Section 3 – Rectification and erasure

Article 14 sets out the data subject's right to rectification, based on Article 12(b) of Directive 95/46/EC.

Article 15 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the right to obtain erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology “blocking”.

---

[31] Adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2011. Cf. also Article 13(3) of the proposal for a Regulation on a Common European Sales Law (COM(2011)635final.

Article 16 introduces the data subject's right to data portability, i.e. to transfer data from one automated processing system to and into another, without being prevented from doing so by the controller. As a precondition, it provides the right to obtain from the controller those data in a commonly used format.

3.4.3.4. Section 4 – Right to object and profiling

Article 17 provides the data subject's rights to object. It is based on Article 14 of Directive 95/46/EC, with some modifications, including as regards the burden of proof and its application to non-commercial direct marketing, in contrast to Article 5(2) which provides that for purposes of commercial direct marketing the data subject's consent is required to make the processing lawful.

Article 18 concerns the data subject's right not to be subject to a measure based on profiling. It builds on, with modifications and additional safeguards, Article 15(1) of Directive 95/46 on automated individual decisions, and takes account of the Council of Europe's recommendation on profiling[32].

3.4.4. CHAPTER IV - CONTROLLER AND PROCESSOR

3.4.4.1. Section 1 – General obligations

Article 19 takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance.

Article 20 sets out the obligations of the controller arising from the principles of data protection by design and by default.

Article 21 on joint controllers clarifies the responsibilities of joint controllers as regards their internal relationship and towards the data subject.

Article 22 obliges controllers not established in the Union, where the Regulation applies to their processing activities, to designate a representative in the Union.

Article 23 clarifies the position and obligation of processors, partly based on Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller.

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

Article 25 introduces the obligation for controllers and processors to maintain documentation of the 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 clarifies the obligations for the co-operation with the supervisory authority.

---

[32] CM/Rec (2010)13.

3.4.4.2. Section 2 – Data security

Article 27 obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC and extending that obligation to processors, irrespective of the contract with the controller.

Articles 28 and 29 introduce an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.

3.4.4.3. Section 3 – Data protection assessment and prior authorisation

Article 30 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

Article 31 concerns the cases where authorisation by, and consultation of, the supervisory authority is mandatory prior to the processing building on the concept of prior checking in Article 20 of Directive 95/46/EC.

3.4.4.4. Section 4 – Data protection officer

Article 32 introduces a mandatory data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring. This builds on Article 18(2) of Directive 95/46/EC which provided the possibility for Member States to introduce such requirement as a surrogate of a general notification requirement.

Article 33 sets out the position of the data protection officer.

Article 34 provides the core tasks of the data protection officer.

3.4.4.5. Section 5 – Codes of conduct and certification

Article 35 concerns codes of conduct, building on the concept of Article 27(1) of Directive 95/46/EC and clarifying the content of the codes and the procedures.

Article 36 newly introduces the possibility to establish certification mechanisms and data protection seals and marks.

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

Article 37 contains the general principles for data transfers to third countries or international organisations, including onward transfers.

Article 38 sets out the criteria, conditions and procedures for the adoption of an adequacy decision by the Commission, based on Article 25 of Directive 95/46/EC. The criteria for the Commission's assessment of an adequate or not adequate level of protection include expressly the rule of law, judicial redress and independent supervision. The article now confirms explicitly the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country.

Article 39 requires for transfers to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically introduced in the legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorisation by supervisory authorities.

Article 40 describes in further detail the conditions for transfers by way of binding corporate rules, based on the current practices and requirements from supervisory authorities.

Article 41 spells out and clarifies the derogations for a data transfer, based on the existing provisions of Article 26 of Directive 95/46/EC. In addition, a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of that transfer operation.

Article 42 clarifies that in accordance with international public law and existing EU legislation, in particular Council Regulation (EC) No 2271/96[33], a controller operating in the EU is prohibited to disclose personal to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority.

Article 43 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 Recommendation by the Organisation for Economic Co-operation and Development (OECD) on cross-border co-operation in the enforcement of laws protecting privacy of 12 June 2007.

Article 44 newly 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 45 obliges Member States to establish supervisory authorities, based on Article 28(1) of Directive 95/46/EC and enlarging the mission to co-operation with each other and with the Commission.

Article 46 clarifies the conditions for the independence of supervisory authorities, implementing case law by the Court of Justice of the European Union[34], inspired also by Article 44 of Regulation (EC) No 45/2001[35].

---

33 Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, OJ L 309, 29.11.1996, p.1.

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

Article 47 provides general conditions for the members of the supervisory authority, implementing the relevant case law[36] and inspired also by Article 42(2)-(6) of Regulation (EC) 45/2001.

Article 48 sets out rules on the establishment of the supervisory authority to be provided by the Member States by law

Article 49 lays down professional secrecy of the members and staff of the supervisory authority is based on Article 28(7) of Directive 95/46/EC.

3.4.6.2. Section 2 – Duties and powers

Article 50 sets out the competence of the supervisory authorities. The general rule, based on Article 28(6) of Directive 95/46/EC (competency on the territory of its own Member State), is complemented by the new competence as lead authority in case that a controller or processor is established in several Member States, to ensure unity of application ('one-stop shop'). 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 51 provides the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public on risk, rules, safeguards and rights.

Article 52 provides the powers of the supervisory authority, in parts building on Article 28(3) of Directive 95/46/EC and Article 47 of Regulation (EC) 45/2001, and adding some new elements, including the power to sanction administrative offences.

Article 53 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 AND CONSISTENCY; EUROPEAN DATA PROTECTION BOARD

3.4.7.1. Section 1 – Co-operation

Article 54 introduces explicit rules on mandatory mutual assistance, including consequences for non-compliance with the request of another supervisory, building on Article 28 (6)2 of Directive 95/46/EC.

Article 55 introduces rules on joint operations, inspired by Article 17 of Council Decision 2008/615/JHA[37], including a right of supervisory authorities to participate in such operations.

3.4.7.2. Section 2 – Consistency

Article 56 introduces a consistency mechanism for ensuring unity of application in relation to processing operations which may concern data subjects in several Member States.

---

35 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.

36 op. cit, footnote 33..

37 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.

Article 57 sets out the procedures and conditions for an opinion of the European Data Protection Board.

Article 58 concerns Commission opinions on matters dealt within the consistency mechanism, which may either reinforce the opinion of the European Data Protection Board or express a divergence with that opinion, and the draft measure of the supervisory authority.

Article 59 concerns Commission decisions requiring the competent authority to suspend its draft measure when this is necessary to ensure the correct application of this Regulation.

Article 60 provides for a possibility for the adoption of provisional measures, in an urgency procedure.

Article 61 sets out the requirements for Commission implementing acts under the consistency mechanism.

Article 62 provides the obligation for the enforcement of measures of a supervisory authority in all Member States concerned, and sets out that the application of the consistency mechanism is precondition for the legal validity and enforcement of the respective measure.

3.4.7.3. Section 3 – European Data Protection Board

Article 63 establishes the European Data Protection Board, consisting of the heads of the supervisory authority of each Member State and of the European Data Protection Supervisor, The European Data Protection Board replaces the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC. It is clarified that the Commission is not a member of the European Data Protection Board but has the right to participate in the activities and to be represented.

Article 64 underlines and clarifies the independence of the European Data Protection Board.

Article 65 describes the tasks of the European Data Protection Board, based on Article 30(1) of Directive 95/46/EC, and provides for additional elements, reflecting the increased scope of activities of the European Data Protection Board, within the Union and beyond. In order to be able to react in urgent situations, it provides the Commission with the possibility to ask for an opinion within a specific time-limit.

Article 66 requires the European Data Protection Board to report annually on its activities, building on Article 30(6) of Directive 95/46/EC.

Article 67 sets out the European Data Protection Board's decision making procedures, including the obligation to adopt rules of procedure which should extend also to operational arrangements.

Article 68 contains the provisions on the chair and on the deputy chairs of the European Data Protection Board.

Article 69 sets out the duties of the chair as well as the duration of the terms of office.

Article 70 establishes the secretariat of the European Data Protection Board at the European Data Protection Supervisor and specifies its tasks.

Article 71 provides for rules on the confidentiality.

Article 72 sets out the applicable rules for access to documents of the European Data Protection Board.

3.4.8. CHAPTER VIII - REMEDIES, LIABILITY AND SANCTIONS

Article 73 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. It specifies also the bodies, organisations or associations which may lodge a complaint on behalf of the data subject or, in case of a personal data breach, on its own behalf.

Article 74 concerns the right of judicial remedy against a supervisory authority. It builds on the general provision of Article 28(3) of Directive 95/46/EC and provides specifically a judicial remedy for obliging the supervisory authority to act on a complaint, and that the proceedings can be brought either before the court of the supervisory authorities' Member State or before the court of the Member State in which the data subject is residing.

Article 75 concerns the right to a judicial remedy against a controller or processor, building on Article 22 of Directive 95/46/EC, and providing a choice to go to court in the Member State where the defendant is established or where the data subject is residing. Where proceedings concerning the same matter are pending in the consistency mechanism, the court may suspend its proceedings, except in case of urgency.

Article 76 lays down 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 the information of the courts on parallel proceedings in another Member State, and the possibility for the courts to suspend in such case the proceedings.[38] There is an obligation on Member States to ensure rapid court actions.[39]

Article 77 sets out the right to compensation and liability. It builds on Article 23 of Directive 95/46/EC, extends this right to damages caused by processors and clarifies the liability of joint controllers and joint processors.

Article 78 obliges Member States to lay down rules on penalties, to sanction infringements of the Regulation, and to ensure their implementation.

Article 79 obliges each supervisory authority to sanction the administrative offences listed in the catalogues set out in this provision, imposing fines between the minimum and maximum amounts, with due regard to circumstances of each individual case.

---

38 Building on Article 5(1) of 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; and Article 13(1) of 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 Building on Article 18(1) of 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.

3.4.9. CHAPTER IX - PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80 empowers Member States to act as concerns the relationship to the right of freedom of expression. It is based on Article 9 of Directive 95/46/EC, as interpreted by the Court of Justice of the EU.[40]

Article 81 obliges Member States, further to the conditions for special categories of data, to ensure specific safeguards for processing for health purposes.

Article 82 provides an empowerment for Member States to adopt specific laws for processing personal data in the employment context.

Article 83 sets out specific conditions for processing personal data for historical, statistical and scientific research purposes.

Article 84 empowers Member States to adopt specific rules on the access of supervisory authorities to personal data and to premises, where controllers are subject to obligations of secrecy.

Article 85 clarifies the empowerment for the Union or Member States to maintain or introduce restrictions of data subject's rights. This provision is based on Article 13 of Directive 95/46/EC and on the requirements stemming from the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the EU and the European Court of Human Rights.

3.4.10. CHAPTER X - DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86 contains the standard provisions for the exercise of the 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 87 contains the provision for the Committee procedure needed for conferring implementing powers on the Commission in the 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 88 repeals Directive 95/46/EC.

Article 89 determines the relationship to the e-privacy Directive 2002/58/EC.

Article 90 provides the evaluation of the Regulation and related reporting by the Commission.

---

[40] Cf. for the interpretation, e.g. Court of Justice of the EU, judgment of 16 December 2008, Satakunnan Markkinapörssi and Satamedia (C-73/07, ECR 2008 p. I-9831)

Article 91 sets out the date of the entry into force of the Regulation, with a transitional phase of two years as regards the date of its application.

4. BUDGETARY IMPLICATION

The specific budget implications of the proposal relate to task allocated to the European Data Protection Supervisor as specified in the legislative financial statements accompanying this proposal. Specific budgetary implications for the Commission are also assessed in the financial statement accompanying this proposal.

The proposal has implications for the EU's budget.

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)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor[41],

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 and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.

(3) 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[42] seeks to harmonise the protection of fundamental

[41] OJ C , , p. .

[42] OJ L 281 , 23.11.1995, p. 31.

rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. 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, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.

(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.

(7) The objectives and principles of Directive 95/46/EC remain sound, 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 for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. This difference may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(8) In order to ensure consistent and a high level protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should 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.

(9) 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.

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

(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including small and medium-sized enterprises, and for individuals in all Member States with the same level of legally enforceable rights for data subjects and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States.

(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of 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 data concerning them.

(13) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

(14) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data not carried out in the context of the activities of an establishment of a controller in the Union should be subject to the Regulation where the processing activities are directed to data subjects residing in the Union, or serve monitor the behaviour of such data subjects, including for commercial or professional activities, such as offering products and services.

(15) In order to determine whether a processing activity can be considered to be 'directed to' a data subject residing in the Union, it should be ascertained whether it is apparent from the controller's overall activity that the controller was envisaging processing personal data of data subjects residing in the Union, taking account in particular the international nature of the activities, or use of a language or a currency other than the language or currency generally used in the controller's country of establishment with the possibility of making and confirming a reservation in that other language, or the use of a top-level domain name other than that of the country in which the controller is established. On the other hand, the mere accessibility of the controller's website by a data subject residing in the Union is insufficient.

(16) Where the national law of a Member State applies by virtue of international law, the Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(17) 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 Regulation.

(18) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(19) The Regulation should also not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. This exemption should not apply to such personal or domestic activities, where the natural person makes personal data of other natural persons accessible to an indefinite number of individuals, for example via the internet. The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

(20) Within a strong and consistent legislative framework across Union policies, 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, is subject of a specific legal instrument at Union level. Therefore, the Regulation should not apply to the processing activities for those purposes.

(21) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a 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.

(22) 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 Regulation should be applicable to processing involving such data.

(23) When using online services, individuals are associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. Since this leave traces which, combined with unique identifiers and other information received by the servers, can be used to create profiles of the individuals and identify them, this Regulation should be applicable to processing involving such data.

(24) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, based on an affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website and any other statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing carried out for the same purpose or purposes.

(25) The main establishment of a controller or processor should be determined according to objective criteria and implies the effective and real exercise of management activities determining the purposes and means of processing through stable arrangements. The location where the processing is carried out on the basis of such management activities is not the determining factor in this respect.

(26) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

(27) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. To determine when an individual is a child, the Regulation should take over the definition made by the UN Convention on the Rights of the Child.

(28) Any processing of personal data should 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 data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the 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 no longer kept than necessary, time limits should be established by the controller for erasure or for a periodic review.

(29) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law.

(30) Where processing is based on the data subject's consent, the controller should have the burden of proof that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given. In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment, especially where there is a clear imbalance between the data subject and the controller. Consent should not provide a valid legal ground for processing in the public or employment sector.

(31) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law or Member State law which meets the requirements of the EU's Charter of Fundamental Rights for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.

(32) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, without having to state reasons and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by authorities in the performance of their tasks.

(33) Processing should equally be regarded as lawful where it is necessary in the context of a contract or the intended entering into a contract, or to protect an interest which is essential for the data subject's life.

(34) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. In case that the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this further purpose or should base the processing on another 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 Regulation and in particular the information of the data subject on those other purposes should be ensured.

(35) 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 the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(36) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific purposes.

(37) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.

(38) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions; the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(39) The principle of transparency requires that any information, both of the public and of the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.

(40) Modalities should be provided for facilitating the data subject’s exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.

(41) The principles of fair and transparent processing require that the data subject 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.

(42) 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 collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

(43) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. This could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

(44) 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 have 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. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software; however, these considerations should not result that in all information being refused to the data subject.

(45) The controller should use all reasonable measures to verify the identity of a data subject that request access, in particular in the context of online services and online identifiers.

(46) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the processing of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data will be erased and no longer processed, where they have withdrawn their consent for processing or where they object to the processing of personal data concerning them. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later on wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for exercising the right of freedom of expression, when required by law, or where there is a reason to restrict the processing of the data instead of erasing them.

(47) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that any publicly available copies or replications in websites and search engines should also be deleted by the controller who has made the information public.

(48) To further strengthen the control over their own data, data subjects should have the right, where personal data are processed by automated means, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

(49) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be for the controller to demonstrate that his legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

(50) Where personal data are processed for the purposes of direct marketing for non-commercial purposes, the data subject should have the right to object to such processing. In case of direct marketing for commercial purposes, such marketing should be lawful only if the data subject has given prior consent. The consent can be withdrawn.

(51) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

(52) 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 demonstrate the compliance of each processing operation with this Regulation.

(53) 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 Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

(54) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, 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

(55) Where a controller, whose processing activities are directed to data subjects residing in the Union or serve to monitor such data subjects, has no establishment in the Union, the controller should designate a representative, who acts on behalf of the controller and may be addressed by any supervisory authority.

(56) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

(57) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor shall evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, 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.

(58) 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 individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the supervisory authority. The individuals whose personal data 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 of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should include information about measures taken by the controller to address the breach, as well as recommendations for the individual concerned.

(59) 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 law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(60) The general notification requirements set out in Directive 95/46/EC produce administrative and financial burdens. Therefore they should be abolished, in order to ensure effective protection of the rights and freedoms of data subjects by procedures and mechanism which focus instead on those processing operations which are likely to be present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor, which should include in particular contain the envisaged measures, safeguards and mechanisms to ensure the protection of personal data and for demonstrating the compliance with this Regulation.

(61) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as that excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be in a position to be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation may equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

(62) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by an enterprise of a size above micro, small and medium enterprises, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.

(63) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors.

(64) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be

encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(65) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation; the increase in these flows has raised new challenges and concerns with respect to the protection of personal data; however, when personal data are transferred from the Union to third countries or to international organisations, the protection of individuals guaranteed in the Union by this Regulation should continue to be ensured in principle. In any event, transfers to third countries may only be carried out in full compliance with the provisions of this Regulation.

(66) The Commission may decide 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 legal certainty and uniformity throughout the Union. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.

(67) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.

(68) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation 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.

(69) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of protection in a third country by way of appropriate safeguards for the data subject.

(70) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

(71) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(72) Provisions should be made for the possibility for transfers in certain limited circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection on grounds of public interest laid down by Union or Member State law so requires, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer

should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. These possibilities should be interpreted restrictively.

(73) In any case, where the Commission has taken no decision on the adequate level of protection of a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred. In particular, transfers which might be qualified as frequent, massive or structural should only be carried out with the appropriate safeguards with respect to the protection of personal data in a legally binding instrument, such as contractual clauses.

(74) Mutual assistance treaties or international agreements between third countries and the Union or a Member State may provide for the exchange of personal data under specific circumstances, for specific purposes and with appropriate safeguards for the data subjects. However, some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States of the Union. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Consequently, provision should be made to prohibit a controller or processor to directly disclose personal data to requesting third countries, unless authorised to do so by a supervisory authority.

(75) When personal information 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 information. 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 international counterparts.

(76) 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. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(77) This Regulation does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union.

(78) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular

designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.

(79) 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 co-operation with other supervisory authorities throughout the Union.

(80) 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.

(81) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation 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 facilitate 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.

(82) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

(83) The lead authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment. The main establishment should be determined according to objective criteria, such as the controller's or processors central administration within the Union. The central administration is usually the location where the management decisions in relation to the purposes, conditions and means for the processing of personal data are taken. However, this criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore are no determining criteria for a main establishment.

(84) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts 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 to other activities with judges might be involved in accordance with national law.

(85) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally

binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings.

(86) 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.

(87) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.

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

(89) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are directed to, or serve to monitor data subjects in several Member States, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism.

(90) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if it so decides or if so requested by any supervisory authority or the Commission requests.

(91) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.

(92) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

(93) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision. In other cases of cross-border relevance mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

(94) At Union level, a European Data Protection Board should be set up. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this

Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

(95) The Chair of the European Data Protection Board should be a person whose independence is beyond doubt and who is acknowledged as having the experience and skills required to perform the required duties. Therefore the requirements laid down in Article 46(2) to (4), Article 47(2) to (5) and Article 49 in relation to independence, incompatible occupations, data protection experience and professional secrecy should apply mutatis mutandis to the Chair of the European Data Protection Board.

(96) 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 Regulation 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.

(97) 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 with a supervisory authority 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.

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

(99) 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, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.

(100) 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 he proves that he is not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.

(101) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties

(102) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the

minimum and upper limit for the related administrative fines, which shall be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach.

(103) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in so far as this is necessary to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore Member States should adopt legislative measures, laying down the exemptions and derogations necessary for the purpose of balance between these fundamental rights as regards general measures on the lawfulness of the processing of personal data, rights of the data subject, measures on the transfer of data to third countries or international organisations and the power of the supervisory authority. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation;

(104) The processing of data concerning health, including health data as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data for health purposes, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.

(105) The general principles on the protection of individuals with regard to the processing of personal data are also applicable to the employment context. Therefore, in order to ensure respect for workers' fundamental rights and freedoms, in particular their right to protection of personal data, Member States should, within the limits of this Regulation, adopt by law specific rules for the processing of personal data in the employment sector.

(106) The procession of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as guaranteeing patients' rights or on clinical trials.

(107) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt, within the limits of this Regulation, by law specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.

(108) Restrictions on the rights of information, access, rectification, erasure or on the right to object and on certain obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to

safeguard public security, an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(109) In order to fulfil the objectives of this Regulation, 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 movement of personal data 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 lawfulness of processing, change of purpose of processing, processing of special categories of data, procedures and mechanisms for exercising the rights of the data subject, information to the data subject, the right of access, the right to be forgotten and to erasure, measures based on profiling, responsibility of the controller, data protection by design and by default, representatives of controllers not established in the Union, a processor, 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 authorisation and prior consultation, designation and tasks of the data protection officer, codes of conduct, certification, transfers by way of binding corporate rules, transfer derogations, administrative sanctions, processing for health purposes, processing in the employment context and processing for historical, statistical and scientific research purposes. 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.

(110) In order to ensure uniform conditions for the implementation of this Regulation of the modalities for exercising the rights of data subjects, information to the data subject, the right of access, the right to data portability, responsibility of the controller, 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 authorisation and prior consultation, certification, 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, transfers by way of binding corporate rules, disclosures not authorized by Union law, mutual assistance, joint operations, decisions under the consistency mechanism, 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].

(111) The examination procedure should be used for the adoption of the modalities for exercising the rights of data subjects, information to the data subject, the right of

[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.

access, the right to data portability, responsibility of the controller, 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 authorisation and prior consultation, certification, 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, transfers by way of binding corporate rules, disclosures not authorized by Union law, mutual assistance, joint operations, decisions under the consistency mechanism, given that those acts are of general scope.

(112) 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.

(113) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout 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 Regulation does not go beyond what is necessary in order to achieve that objective.

(114) Directive 95/46/EC should be repealed by this Regulation.

(115) As regards Iceland and Norway, this Regulation 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].

(116) As regards Switzerland, this Regulation 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].

(117) As regards Liechtenstein, this Regulation 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].

---

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.

(118) This Regulation 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 freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial.

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and objectives

1. This Regulation lays 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.

2. The objectives of this Regulation are:

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

   (b) to ensure that the free movement of personal data 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 Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union not carried out in the context of the activities of an establishment of a controller in the Union, where the processing activities are directed to such data subjects, or serve to monitor the behaviour of such data subjects.

3. This Regulation applies to the processing of personal data by a controller not established in the Union where the national law of a Member State applies by virtue of international public law.

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

5. This Regulation does 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;

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;

(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity, unless personal data of other natural persons is made accessible to an indefinite number of individuals;

(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Article 3
Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(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 natural or legal person, public authority, agency or any other body 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) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

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

(11) '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;

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

(13) ‘main establishment’ means where the controller’s or the processor's central administration in the Union is located and, in case of the controller, where the purposes, conditions and means of the processing of personal data are determined;

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(15) ‘enterprise’ means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

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

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 45.

CHAPTER II
PRINCIPLES

Article 4
Principles relating to personal data processing

1. 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 6;

(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 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 the compliance with the provisions of this Regulation.

2. Any personal data processed in breach of this Regulation shall no longer be processed.

Article 5
Lawfulness of processing

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

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

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

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

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

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

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where

(i) carried out by public authorities in the performance of their tasks, or

(ii) such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. Processing of personal data for direct marketing for commercial purposes shall be lawful only if the data subject has given consent to the processing of their personal data for such marketing.

3. Processing referred to in points (c) and (e) 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 or must be necessary 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.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

Article 6
Change of purpose of the processing

1. Personal data may only be further processed for another purpose which is compatible with the purposes for which the data were collected, in particular where processing is necessary for historical, statistical or scientific research purposes in accordance with the rules and conditions laid down in Article 83.

2. Where another purpose is not compatible with that for which the personal data are collected, the processing must have a legal basis at least in one of the grounds referred to in Article 5(1)(a) to (e). This shall in particular apply to any change of terms and general conditions of a contract.

3. Personal data collected exclusively for ensuring the security or control of processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of criminal offences.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in paragraph 1 in various sectors and data processing situations, including as regards the processing of personal data related to a child.

Article 7
Conditions for consent

1. The controller shall bear the burden of proving that the data subject has given consent for the processing of their personal data for specified purposes.

2. If the data subject's consent is to be given in the context of a written declaration on another matter, it must be made distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance in the form of dependence between the position of the data subject and the controller.

5. Consent shall not provide a legal basis for the processing

   (a) by public authorities in the performance of their tasks; or

   (b) for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law.

6. Consent of a child shall only be valid when given or authorized by the child's parent or custodian.

Article 8
Processing of special categories of personal data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or offences or criminal convictions or related security measures shall be prohibited.

2. Paragraph 1 shall not apply where:

   (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Article 7, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

   (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so

far as it is authorized by Union law or Member State law providing for adequate safeguards;

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed without the consent of the data subjects;

(e) the processing relates to data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims;

(g) 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;

(h) processing of data concerning health is necessary subject to the conditions and safeguards referred to in Article 80;

(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83.

3. Processing of data relating to administrative sanctions, judgements or offences, criminal convictions or related security measures shall be carried out only under the control of official authority. A register of criminal convictions shall be kept only under the control of official authority.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY AND MODALITIES

Article 9

Transparent information and communication

1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Article 10

Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 12 and for the exercise of the rights of data subjects referred to in Articles 11, and 13 to 17. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Articles 11, 13 to 17. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Articles 11, 13 to 18. 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.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. 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 87(2).

Article 11
Rights in relation to recipients

The data subject shall have the right to obtain from the controller communication to each recipient to whom the data have been disclosed of any rectification or erasure carried out in compliance with Articles 14 and 15. The controller may refuse such communication where this proves impossible or involves a disproportionate effort.

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 12
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

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

   (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on Article 5(1)(b) and the legitimate interests pursued by the controller where the processing is based on Article 5(1)(f);

   (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 or to object to the processing of such personal data;

   (e) the right to lodge a complaint to the supervisory authority referred to in Article 45 and the contact details of the supervisory authority;

   (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 of that third country or international organisation under the rules of that third country or international organisation;

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

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. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

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

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

5. Paragraphs 1 to 4 shall not apply, where:

   (a) the data subject has already the information referred to in paragraphs 1 to 3; or

   (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

   (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further necessary information referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in points (a) and (b) of paragraph 5.

8. 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 sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, confirmation as to whether or not personal data relating to the data subject are being

processed. Where such personal data are being processed, the controller shall provide the following information:

(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 or to object the processing of such personal data;

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

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

(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

2. The data subject shall have the right 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 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3

RECTIFICATION AND ERASURE

Article 14

Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them the processing of which does not comply with this Regulation. 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, including by way of supplementing a corrective statement.

Article 15
Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data where:

   (a) the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed; or

   (b) the data subject withdraws consent on which the processing is based according to Article 5(1)(a), or when the storage period consented to has expired; or

   (c) the data subject objects to the processing of personal data pursuant to Article 17; or

   (d) their processing otherwise does not comply with this Regulation.

   This right shall apply especially in relation to personal data which are made available by the data subject while he or she was a child.

2. Where the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

   (a) for exercising the right of freedom of expression in accordance with Article 79; or

   (b) for historical, statistical and scientific research purposes in accordance with Article 83; or

   (c) for compliance with a legal obligation to retain the data by Union or Member State law to which the controller is subject; this law shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; or

   (d) in the cases referred to in paragraph 4.

4. 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;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 16(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and for a periodic review of the need for the storage of the data are observed.

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

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the criteria for deleting public Internet links, copies or replications of personal data from publicly available communication service as referred to in paragraph 2;

(c) the criteria and conditions as regards personal data identified for the purpose of restricting its processing as referred to in paragraph 4.

Article 16

Right to data portability

1. The data subject shall have the right, where personal data are processed by automated means, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 17
Right to object

1. The data subject shall have the right to object at any time to the processing of personal data which is based on points d), (e) and (f) of Article 5(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing for non-commercial purposes recognised as being in the public interest, the data subject shall have the right to object to the processing of their personal data for such marketing.

3. Where an objection is raised pursuant to paragraph 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

Article 18
Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, creditworthiness, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

   (a) is carried out in the course of the entering into or performance of a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

   (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

   (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Paragraph 2 shall not apply where the processing concerns a child.

4. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based exclusively on the special categories of personal data referred to in Article 8.

5. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 13 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

6. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to point (b) of paragraph 2, by the date specified in Article 90(2) at the latest and, without delay, any subsequent amendment affecting them.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in points (a) to (c) of paragraph 2.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 19
Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation, including the assignment of responsibilities, and the training of staff involved in the processing operations.

2. The measures provided for in paragraph 1 shall in particular include:

   (a) keeping the documentation pursuant to Article 25;

   (b) implementing the data security requirements laid down in Article 27,

   (c) performing a data protection impact assessment pursuant to Article 30;

   (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 31(1) and (2);

   (e) designating a data protection officer pursuant to Article 32(1).

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 measures taken to mitigate such risks.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 4 and as regards the criteria for proportionality under paragraph 4.

6. The Commission may lay down standard forms for the publication of the controllers' rules referred to in paragraph 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 20
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

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 be 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 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 21
Joint controllers

1. Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation by means of an arrangement between them. If this arrangement does not determine

the respective responsibilities in relation to these obligations, the responsibility of those joint controllers to comply with this Regulation shall be solidary.

2. In any case, the data subject may exercise their rights under this Regulation in respect of and against each of the joint controllers.

Article 22

Representatives of controllers not established in the Union

1. Where a controller is not established in the Union, in the situation referred to in Article 2(2), the controller shall designate a representative in the Union.

2. The representative shall be established in one of those Member States where the data subjects to whom the processing activities are directed, or whose behaviour is monitored, reside.

3. The representative designated shall comply with the obligations of the controller laid down in this Regulation.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the designation and functioning of the representative referred to in paragraph 1.

Article 23

Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

   (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 27;

(d) enlist another processor only with the permission of the controller and therefore to 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, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 27 to 31;

(g) hand over all results 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 21.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow to facilitate the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

Article 24

Processing under the authority of the controller and processor

The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Article 25

Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its 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, and of the representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 5(1);

(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 personal data or categories of data relating to them;

(f) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(g) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (d) of Article 39(2) and in point (h) of Article 41(1), the documentation of appropriate safeguards;

(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 19(1);

(j) an indication of the legal basis of the processing operation for which the data are intended, if the controller is a public authority or body.

3. The controller and the processor and, if any, the controller's representative, 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 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

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 87(2).

Article 26

Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 52(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 52(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 27
Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy-by-design and data protection by default.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

   (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.

Article 28
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, as a rule, not later than 24 hours after the personal data breach has been established, notify 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 establishment of a personal data breach.

3. The notification referred to in paragraph 1 must 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 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. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, in addition to the notification referred to in Article 28, communicate 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 referred to in paragraph 1 shall contain at least the information and the recommendations provided for in points (a), (b) and (c) of Article 28(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller 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 data concerned by the personal data breach. Such

technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

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

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3

DATA PROTECTION ASSESSMENT AND PRIOR AUTHORISATION

Article 30

Data protection impact assessment

1. Prior to the processing of personal data, the controller or the processor shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where those 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) an evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's performance at work, creditworthiness, economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and likely to result in measures that produce legal effects concerning the individual or significantly affect the individual; or

   (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases; or

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

(d) personal data in large scale filing systems on children, genetic data or biometric data; or

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to Article 31(2)(b).

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

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. Without prejudice to the protection of commercial or 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 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 31

Prior authorisation and prior consultation

1. The controller or the processor shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with the Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a controller or processor adopts contractual clauses as provided for in Article 39(2)(d) for the transfer of personal data to a third country or an international organisation; or

(b) a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data as referred to in Article 42(1).

2. The controller or processor shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended

processing with the Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 30 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

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

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

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involve processing activities that are directed to, or serve to monitor the behaviour of, data subjects in another Member State or other Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 56 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 30 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.

7. 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 with the Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (b) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4

DATA PROTECTION OFFICER

Article 32

Designation of the data protection officer

1. The controller or the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body; or

   (b) the processing is carried out by an enterprise employing more than 250 persons permanently; or

   (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects; or

2. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

3. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 34. 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.

4. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

5. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed from the post of the data protection officer, if they no longer fulfil the conditions required for the performance of their duties.

6. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

7. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

8. The controller or the processor shall communicate the name and contact details of the data protection officer to data subjects pursuant to Article 12(1)(a). Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject’s data and to request exercising the rights under this Regulation.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 2.

Article 33
Position of the data protection officer

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

2. The controller or processor shall ensure that the data protection officer performs their 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 34.

Article 34
Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

   (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

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

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

   (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 28 and 29;

   (f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 30 and 32;

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

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

SECTION 5

CODES OF CONDUCT AND CERTIFICATION

Article 35
Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;

(b) the collection of data;

(c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 72 and 74.

2. Associations and other bodies representing categories of controllers or processors which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in a Member State. The supervisory authority may give an opinion whether the draft code of

conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects on these drafts.

3. Associations and other bodies representing categories of controllers may submit draft Union codes of conduct and amendments or extensions to existing Union codes of conduct to the Commission.

4. The Commission may adopt implementing acts for deciding that the Union codes of conduct and amendments or extensions to existing Union codes of conduct submitted to it have general validity. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 36
Certification

1. The Member States and the Commission shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for bestowal, and deprivation and requirements for recognition within the Union and in third countries.

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

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 37
General principles for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if:

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

(b) the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation; and

(c) the other provisions of this Regulation are complied with by the controller and processor.

Article 38
Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

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 professional rules and security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those 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 subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

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

3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

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 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 87(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 87(3).

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 39 to 41. 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 and international organisations 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 39

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 38, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. These appropriate safeguards referred to in paragraph 1 shall be provided for by:

   (a) binding corporate rules in accordance with Article 40; or

   (b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

   (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 56 when declared generally valid by the Commission pursuant to point (b) of Article 60(1); or

   (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 the controller or processor shall obtain prior authorisation of the contractual clauses according to Article 31(1)(a) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism set out in Article 56.

Article 40

Transfers by way of binding corporate rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 56 approve binding corporate rules, provided that they

   (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;

   (b) expressly confer enforceable rights on data subjects;

   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

   (a) the structure and contact details of the group of undertakings and its members;

   (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

   (c) their binding nature, both internally and externally;

   (d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;

   (e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 18, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 74(2) , and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

   (f) the acceptance by the controller or processor established on the territory of a Member State of the Union of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) is provided to the data subjects in accordance with Article 9;

(h) the tasks of the data protection officer designated in accordance with Article 32, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules.

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i).

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 41
Derogations

1. In the absence of an adequacy decision pursuant to Article 38 or of appropriate safeguards pursuant to Article 39, 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 data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for grounds of public interest, or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, cannot be qualified as frequent, massive or structural and the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.

4. Points (a), (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the performance of their tasks.

5. Processing based on points (d), (e), (f) and (g) of paragraph 1 must have a legal basis in Union law, or the law of the Member State to which the controller is subject, 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.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in paragraph 1 (h) in the documentation referred to in Article 25 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Article 42

Disclosures not authorized by Union law

1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.

2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer by the supervisory authority in accordance with point (b) of Article 31(1).

3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of paragraph 1 and paragraph 5 of Article 41.

4. The supervisory authority shall inform the competent national authority of the request. The controller or processor shall also inform the data subject of the request and of the authorisation by the supervisory authority.

5. The Commission may lay down the standard format of the notifications to the supervisory authority referred to in paragraph 2 and the information of the data subject referred to in paragraph 4 as well as the procedures applicable to the notification and information. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 43

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities 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 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 38(3).

Article 44
Report by the Commission

The Commission shall submit a report on the application of Articles 37 to 43 to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. For that purpose, the Commission may request information from the Member States and supervisory authorities. The Member States and the supervisory authorities shall supply this information without undue delay. The report shall be made public.

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 45
Supervisory authority

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

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraphs 1 and 2, by the date specified in Article 90(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 46
Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, 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 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 has 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.

8. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraphs 5 to 7, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 47
General conditions for the members of the supervisory authority

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

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties 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 other benefits in its stead by the competent national court, if the member no longer fulfils the

conditions required for the performance of the duties or is guilty of serious misconduct.

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

6. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 48
Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law within the limits of this Regulation:

   (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 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 Regulation, 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.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 49
Professional secrecy

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

SECTION 2
DUTIES AND POWERS

Article 50
Competence

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

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the Member State where the main establishment of the controller or processor is located shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, applying the provisions of mutual assistance and co-operation referred to in Articles 54, 55 and 56.

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

Article 51
Duties

1. The supervisory authority shall:

   (a) monitor and ensure the application of this Regulation;

   (b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 71, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

   (c) provide mutual assistance and ensure the consistency of application and enforcement of this Regulation;

   (d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the inquiries within a reasonable period;

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

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

(g) authorise and be consulted on the processing operations referred to in Article 31;

(h) decide on the draft codes of conduct pursuant to Article 35;

(i) approve binding corporate rules pursuant to Article 40;

(j) participate 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 Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

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

5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are manifestly 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 the manifestly excessive character of the request.

Article 52
Powers

1. Each supervisory authority shall have 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 provided by this Regulation, including Articles 14 to 17;

(c) to order the controller or the processor to provide the information pursuant to Articles 9, 11, 12, 28 and 29;

(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 31;

(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 of this Regulation 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 duties;

(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 this Regulation is being carried out there, without prejudice to a judicial authorisation required by national law.

3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, including to bring an action to the competent court pursuant to Article 75(2).

4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 77(2), (3) and (4).

Article 53
Activity report

Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 54
Mutual assistance

1. Supervisory authorities shall provide each other mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take 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 Regulation without delay and no 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 of this Regulation.

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. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with

Article 50(1) and shall submit the matter to the European Data Protection Board in the procedure set out in Article 56.

9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 55
Joint operations

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

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

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

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 50(1).

6. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism set out in Article 56.

SECTION 2
CONSISTENCY

Article 56
Consistency mechanism

For the purposes set out in Article 45(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.

Article 57
Opinion by the European Data Protection Board

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

   (a) relates to processing activities which are directed to, or serve to monitor the behaviour of, data subjects in another Member State or other Member States; or

   (b) may substantially affect the free movement of personal data within the Union; or

   (c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 31(5); or

   (d) aims to determine standard data protection clauses referred to in Article 39(2)(a); or

   (e) aims to authorise contractual clauses referred to in Article 39(2)(c) for transfers to third countries or international organisations; or

   (f) aims to approve binding corporate rules within the meaning of Article 40.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in this mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 54 or joint operation in accordance with Article 55.

4. The Commission may request that any matter shall be dealt with in this mechanism if necessary to ensure correct and consistent application of this Regulation.

5. The supervisory authority shall electronically communicate any relevant information, including a summary of the case, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to in paragraph 1 and the Commission of the opinion and make the opinion public.

8. The supervisory authority referred to in paragraph 1 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure to the chair of the European Data Protection Board and to the Commission, using a standardised format.

Article 58
Opinion by the Commission

1. Within ten weeks after the communication referred to in Article 57(1), or at the latest within six weeks in the case of Article 60, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters communicated by supervisory authorities pursuant to Article 57 or 60, or which should have been communicated.

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.

4. Where the supervisory authority intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a reasoned

justification. In this case the draft measure shall not be adopted for one further month.

Article 59
Suspension of a draft measure

1. Within one month after the communication referred to in Article 58(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of the Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Articles 57(7) or 60(2), where it appears necessary in order to:

   (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or

   (b) adopt a measure pursuant to point (a) of Article 61(1).

2. The Commission shall specify the duration of the suspension which shall not exceed 12 months .

3. During the periods referred to in paragraph 2, the draft measure shall not be adopted by the supervisory authority.

Article 60
Urgency procedure

1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure set out in Article 56, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such urgent opinion, including for the urgency of final measures.

3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measures in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such urgent opinion, including for the urgent need to act.

4. In derogation from Article 57(7), an urgent opinion referred to in paragraphs 2 and 3 shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 61
Implementing acts

1. The Commission may adopt implementing acts for:

   (a) ensuring the consistent application of this Regulation in relation to matters communicated by supervisory authorities pursuant to Article 57 or 60, or which should have been communicated;

   (b) deciding, within the period referred to in Article 58(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 57(2), as having general validity;

   (c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;

   (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraphs 5, 6 and 8 of Article 56.

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) and shall also take account of the opinion issued by the European Data Protection Board.

2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.

3. The absence or adoption of a measure as referred to in paragraphs 1 or 2 or in Articles 58 and 59 does not prejudice any other measure by the Commission under the Treaties.

Article 62
Enforcement

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

2. Where a supervisory authority does not submit a draft measure to the consistency mechanism contrary to paragraphs (2) to (5) of Article 56, the measure of the supervisory authority shall not be legally valid and enforceable.

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 63
European Data Protection Board

1. A European Data Protection Board is hereby set up.

2. The European Data Protection Board shall be composed of a head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Article 64
Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 65 and 66.

2. Without prejudice to requests by the Commission referred to in Articles 65(1) and (2), the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

Article 65
Tasks of the European Data Protection Board

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the Advisory Body shall, on its own initiative or at the request of the Commission, in particular:

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

   (b) examine, on request of the Commission or on the own initiative of the European Data Protection Board or of one of its members, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism set out in Article 56;

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

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

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

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's shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 86 and make them public.

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

Article 66
Reports

1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.

The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 65(1).

2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

Article 67
Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its members.

2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements, including to provide for the continuation

of exercising duties when a member's term of office expires or a member resigns, the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 56.

Article 68

Chair of the European Data Protection Board

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor unless he or she has been elected chair.

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable. If the head of a supervisory authority of a Member State is elected as chair, his or her function as head of a supervisory authority shall be suspended for the term of his or her office as chair of the European Data Protection Board.

3. The Commission shall determine the regulations and general conditions governing the performance of the chair's duties and in particular his or her salary, allowances and any other benefits in lieu of remuneration.

Article 69

Tasks of the chair of the European Data Protection Board

1. The chair shall have the tasks:

   (a) to represent the European Data Protection Board;

   (b) to convene the meetings of the European Data Protection Board and prepare its agenda;

   (c) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 56.

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

Article 70

Secretariat of the European Data Protection Board

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall host that secretariat.

2. The secretariat shall provide high-quality analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.

3. The secretariat shall be responsible in particular for:

   (a) the day-to-day business of the European Data Protection Board

(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;

(c) the use of electronic means for the internal and external communication;

(d) translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection Board;

(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

4. The secretariat shall be provided with the human, technical and financial resources necessary for the effective performance of its tasks.

Article 71
Confidentiality

1. The European Data Protection Board discussions shall be confidential.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents pursuant to Article 72 or the European Data Protection Board otherwise makes them public.

3. The members of the committee, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

Article 72
Access to documents

Requests for access to documents of the European Data Protection Board shall be handled in accordance with Regulation No 1049/2001[47] regarding public access to European Parliament, Council and Commission documents.

[47] OJ L145, 31.05.2001, page 43.

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

Article 73
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.

3. Any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State also on its own behalf, if it considers that Articles 28 or 29 have been infringed as a result of the processing of personal data.

Article 74
Right to a judicial remedy against a supervisory authority

1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint, in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to Article 51(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. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 75
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 as referred to in Article 73, every

person shall have the right to a judicial remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

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

3. Where proceedings are pending in the consistency mechanism referred to in Article 56, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

4. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 76
Common rules for court proceedings

1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Article 74 and 75 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 of this Regulation or to ensure consistency of the protection of personal data within the Union.

3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.

4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may 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 77
Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

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 the processor proves that they are not responsible for the event giving rise to the damage.

Article 78
Penalties

1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.

2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 79
Administrative sanctions

1. Without prejudice to other sanctions and remedies, each supervisory authority shall sanction at least the administrative offences listed in paragraphs 2 to 4.

2. The supervisory authority shall impose a fine between 100 EUR and 300 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

   (a) does not provide the mechanisms for requests by data subjects or does not respond timely or not in the required format to data subjects pursuant to Articles 10(1) and (2);

   (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 10(4);

   (c) does not report on internal policies pursuant Article 19(5).

3. The supervisory authority shall impose a fine between 500 EUR and 600 000 EUR, or in case of an enterprise up to 3 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Articles 9, 10(3) and 12;

(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 13 and 14 or does not communicate the relevant information to a recipient pursuant to Article 11;

(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not erase any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in a publicly available communication service pursuant Article 15;

(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 16;

(e) does not comply with a objection or the requirement pursuant to Article 17;

(f) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 21(1);

(g) does not or not sufficiently maintain the documentation pursuant to Articles 25 28(4), 39(3) or 41(3);

(h) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

4. The supervisory authority shall impose a fine between 100 000 EUR and 1 000 000 EUR or, in case of an enterprise up to 5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 5, 6 and 7;

(b) processes special categories of data in violation of Articles 8 and 80;

(c) does not comply with the conditions in relation to measures based on profiling pursuant to Article 18;

(d) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 19, 20 and 27;

(e) does not designate a representative pursuant to Article 22;

(f) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 23 and 24;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 28 and 29;

(g) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 30 and 31;

(h) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 32, 33 and 34;

(i) misuses a data protection seal or mark in the meaning of Article 36;

(j) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by a adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 37 to 42;

(k) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 52(1);

(l) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Articles 25(3), 26, 31(4) and 52(2);

(m) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

5. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 20 and the degree of co-operation with the supervisory authority in order to remedy the breach. It must exceed the financial benefit to the perpetrator derived from the administrative offence.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 2, 3 and 4, taking into account the criteria referred to in paragraph 5.

CHAPTER IX

PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80

Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on the transfer of personal data to third countries and international organisations in Chapter V and the independent supervisory authorities in Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 81

Processing for health purposes

1. Within the limits of this Regulation and in particular in accordance with Article 8, and subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals, Member States shall ensure that data concerning health may be processed only if processing of those data is necessary for:

   (a) the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies;

   (b) other reasons of public interest in areas such as public health and social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 82

Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules to ensure respect for workers' fundamental rights and freedoms, in particular their right to protection of their personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 83

Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

   (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

   (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

2. Bodies conducting historical, statistical or scientific research may publish personal data only if:

   (a) the data subject has given consent, subject to the conditions laid down in Article 7; or

   (b) the publication of personal data is necessary to present research findings and the interests or the fundamental rights or freedoms of the data subject do not override the interests of research; or

   (c) the data subject has made the data public.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data

subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Article 84
Obligations of secrecy

1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 52 (2) in relation to controllers or processors that are subject under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, only if they are necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission of the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 85
Restrictions for objectives of public interest

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 9 to 18, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard the following public interests of the Union and of the Member States:

   (a) public security;

   (b) an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters;

   (c) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a) and (b);

   (d) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 shall contain explicit and detailed provisions at least as to:

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

   (b) the personal data to be processed;

   (b) the specific purposes and means of processing;

   (c) the determination of the controller, or the specific criteria for his nomination;

   (e) the natural persons authorised to process the data;

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

(g) the use that may be made of the information thus obtained;

(h) safeguards against arbitrary interferences by public authorities, such as the scope of any discretion, if any, conferred to the competent authorities;

(i) the supervision of the processing activities by an independent authority.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

CHAPTER X

DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86
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 5(4), 6(4), 8(4), 10(5), 12(7), 13(3), 15(8), 18(7), 19(6), 20(3), 22(5), 23(5), 25(4), 27(3), 28(5), 29(5), 30(6), 32(8), 33(9), 35(4), 36(2), 40(3), 41(7), 79(6), 81(3), 82(2), 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in Articles 5(4), 6(4), 8(4), 10(5), 12(7), 13(3), 15(8), 18(7), 19(6), 20(3), 22(5), 23(5), 25(4), 27(3), 28(5), 29(5), 30(6), 32(8), 33(9), 35(4), 36(2), 40(3), 41(7), 79(6), 81(3), 82(2), 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of 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 Articles 5(4), 6(4), 8(4), 10(5), 12(7), 13(3), 15(8), 18(7), 19(6), 20(3), 22(5), 23(5), 25(4), 27(3), 28(5), 29(5), 30(6), 32(8), 33(9), 35(4), 36(2), 40(3), 41(7), 79(6), 81(3), 82(2), 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Article 87
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 88
Repeals

1. Directive 95/46/EC shall be repealed.

2. References to the repealed Directive shall be construed as references to this Regulation.

Article 89
Relationship to Directive 2002/58/EC

Article 88(2) shall apply also in relation to Directive 2002/58/EC, whereby the reference in Article 15(2) of Directive 2002/58 to Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall be construed as reference to Articles 72 to 77 of this Regulation.

Article 90
Evaluation

The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Regulation and aligning other legal instruments. The reports shall be made public.

Article 91
Entry into force and application

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

2. It shall apply as from two years from the date referred to in paragraph 1.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

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

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned in the ABM/ABB structure

1.3. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact

1.7. Management method(s) envisaged

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on operational appropriations

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party participation in financing

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and the Council on general rules for the Protection of Individuals with regard to the processing of personal data and on the free flow of personal data

1.1. Policy area(s) concerned in the ABM/ABB structure[48]

Area of Freedom, Justice and Security – Protection of Personal Data

The budgetary impact concerns the Commission and the EDPS. The impact on the Commission budget is detailed in the tables of this financial statement. The elements concerning the EDPS are shown in the Annex.

1.2. Nature of the proposal/initiative

☑ The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[49]

☐ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.3. Objectives

1.3.1. The Commission's multiannual strategic objective(s) targeted by the proposal/initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and put individuals in control of their data, particularly in the context of technological developments and increased globalisation;

- enhancing the internal market dimension of data protection, by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

---

48 ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

49 As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

1.3.1. Specific objective(s) and ABM/ABB activity(ies) concerned

Specific objective No 1

To ensure consistent enforcement of data protection rules

Specific objective No 2

To rationalise the current governance system to help ensuring a more consistent enforcement

ABM/ABB activity(ies) concerned

[…]

1.3.2. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

As regards data controllers, both public and private entities shall benefit from more legal certainty by harmonised and clarified EU data protection rules and procedures creating a level playing field and ensuring consistent enforcement of data protection rules, as well as a considerable reduction of administrative burden.

Individuals will enjoy better control of their personal data and trust the digital environment and will remain protected including when their personal data are processed abroad. They will also encounter reinforced accountability of those processing personal data.

A comprehensive data protection system will also cover the areas of police and justice, including and beyond the former 3rd pillar.

1.3.3. Indicators of results and impact

Specify the indicators for monitoring implementation of the proposal/initiative.

(cf. Impact Assessment, Section 8)

Indicators shall be evaluated periodically and shall include the following elements:

- Time and costs spent by data controllers complying with legislation in 'other Member States'
- Resources allocated to DPAs,
- established DPOs in public and private organisations,
- Use made of DPIA
- number of complaints made by data subjects and compensation received by data subjects
- number of cases leading to prosecution of data controllers
- fines imposed on data controllers responsible for breaches of data protection.

1.4. Grounds for the proposal/initiative

1.4.1. Requirement(s) to be met in the short or long term

The current divergences in the implementation, interpretation and enforcement of the Directive by Member States ***hamper the functioning of the internal market and co-operation between public authorities in relation to EU policies.*** This goes against the fundamental objective of the Directive of facilitating the free flow of personal data in the internal market. The rapid development of new technologies and globalisation further exacerbates this problem.

Individuals enjoy different data protection rights, due to fragmentation and inconsistent implementation and enforcement in different Member States. Furthermore, ***individuals are often neither aware nor in control of what happens to their personal data*** and therefore fail to exercise their rights effectively.

1.4.1. Added value of EU involvement

Member States cannot alone reduce the problems in the current situation. This is particularly the case for those problems that arise from the fragmentation in national legislations implementing the EU data protection regulatory framework. Thus, there is a strong rationale for the legal framework for data protection being at the EU level. There is a particular 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 to all individuals across the EU.

1.4.2. Lessons learned from similar experiences in the past

The present proposals build on the experience with Directive 95/46/EC and the problems encountered due to the fragmented transposition and implementation of that Directive which have blocked it form achieving both its objective, i.e. a high level of data protection and a single market for data protection.

1.4.3. Coherence and possible synergy with other relevant instruments

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level - technologically neutral, and future proof for the decades to come. It will benefit individuals – by strengthening their data protections rights, particularly in the digital environment - and will simplify the legal environment for businesses and the public sector, thus stimulating the development of the digital economy across the EU internal market and beyond, in line with the objectives of the Europe 2020 strategy.

The core of the data protection reform package consists of:

– a Regulation replacing Directive 95/46/EC;

– a Directive on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

These legislative proposals are accompanied by a report on the implementation by Member States of what is currently the main EU data protection instrument in the areas of police co-

operation and judicial co-operation in criminal matters, the Framework Decision 2008/977/JHA , and - to ensure the necessary consistency with the EU Data Protection Reform - a Recommendation from the Commission to the Council to authorise the opening of negotiations with a view to modernising the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) , which is also currently being revised.

1.5. Duration and financial impact

☐ Proposal/initiative of **limited duration**

1. ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

2. ☐ Financial impact from YYYY to YYYY

☑ Proposal/initiative of **unlimited duration**

1. Implementation with a start-up period from 2014 to 2016,

2. followed by full-scale operation.

1.6. Management mode(s) envisaged[50]

☑ **Centralised direct management** by the Commission

☐ **Centralised indirect management** with the delegation of implementation tasks to:

3. ☐ executive agencies

4. ☐ bodies set up by the Communities[51]

5. ☐ national public-sector bodies/bodies with public-service mission

3. ☐ persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation

☐ **Shared management** with the Member States

☐ **Decentralised management** with third countries

☐ **Joint management** with international organisations ***(to be specified)***

If more than one management mode is indicated, please provide details in the "Comments" section.

Comments

//

[50] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[51] As referred to in Article 185 of the Financial Regulation.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The first evaluation will take place 3 years after the entry into force of the legal instruments. An explicit review clause, by which the Commission will evaluate the implementation, is included in the legal instruments. The Commission will subsequently report to the European Parliament and the Council on its evaluation. Further evaluations will have to take place every four years. The Commission methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted studies on the implementation of the legal instruments, questionnaires to national data protection authorities, expert discussions, workshops, Eurobarometer, and so forth.

2.1. Management and control system

2.1.1. Risk(s) identified

An Impact Assessment has been carried out for the reform the data protection framework in the EU to accompany the proposals for the Regulations and the Directive

The new legal instrument will introduce a consistency mechanism, ensuring that independent supervisory authorities in MS apply the framework in a consistent and coherent manner. The mechanism will operate through a body composed of the national authorities, which will replace the current Article 29 Working Party. The European Data Protection Supervisor will provide the secretariat to this body.

In case of possibly divergent decisions by MS authorities, the body is consulted in order to find a common agreement. Should this procedure fail to produce a result, or if a national authority refuses to comply with the common result, the Commission will have the responsibility to ensure that EU legislation is complied with and may issue Recommendations or adopt a Decision on the case.

The consistency mechanism requires additional resources at the EDPS (12 FTE and adequate administrative and operative appropriations, e.g., for IT systems and operations) for providing the secretariat and at the Commission (5 FTE and related administrative and operational appropriations) for the handling of consistency cases.

2.1.1. Control method(s) envisaged

Existing control methods applied at EDPS and Commission respectively will cover the additional appropriations.

2.2. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

Existing fraud prevention measures applied at EDPS and Commission will cover the additional appropriations.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

1. Existing expenditure budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Description……...…….]	Diff./non-diff. (52)	from EFTA[53] countries	from candidate countries[54]	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
3a	33 01 04 01 Section IX EDPS Titles 1 1 Staff and 2	Diff/non-diff.	NO	NO	NO	NO

52 Diff. = Differentiated appropriations / Non-diff. = Non-Differentiated Appropriations

53 EFTA: European Free Trade Association.

54 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3.1. Estimated impact on expenditure

3.1.1. Summary of estimated impact on expenditure

EUR million (to 3 decimal places)

Heading of multiannual financial framework:	Number	3a

DG: JUST			Year **N**[55]**= 2014**	Year **N+1**	Year **N+2**	Year **N+3**	… enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
• Operational appropriations										
Number of budget line 33 01 04 01	Commitments	(1)	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
	Payments	(2)	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
Number of budget line	Commitments	(1a)								
	Payments	(2a)								
Appropriations of an administrative nature financed from the envelope for specific programmes[56]										
Number of budget line		(3)								
TOTAL appropriations for DG JUST	Commitments	=1+1a +3	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
	Payments	=2+2a +3	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**

• TOTAL operational appropriations	Commitments	(4)	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
	Payments	(5)	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING 3a of the multiannual financial framework	Commitments	=4+ 6	0.650	1.450	1.600	1.650	1.650	1.650	1.650	10.300
	Payments	=5+ 6	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**

55 Year N is the year in which implementation of the proposal/initiative starts.

56 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

If more than one heading is affected by the proposal / initiative:

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADINGS 1 to 4 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**
	Payments	=5+ 6	0.650	1.450	1.600	1.650	1.650	1.650	1.650	**10.300**

Heading of multiannual financial framework:	**5**	" Administrative expenditure "

EUR million (to 3 decimal places)

		Year **N= 2014**	Year **N+1**	Year **N+2**	Year **N+3**	… enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
DG: JUST									
• Human resources		0.318	0.636	0.89	1.081	1.081	1.081	1.081	6.168
• Other administrative expenditure		0.035	0.070	0.098	0.119	0.119	0.119	0.119	0.678
TOTAL DG JUST		**0.353**	**0.706**	**0.988**	**1.200**	**1.200**	**1.200**	**1.200**	**6.846**

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	**0.353**	**0.706**	**0.988**	**1.200**	**1.200**	**1.200**	**1.200**	**6.846**

EUR million (to 3 decimal places)

		Year **N**[57]	Year **N+1**	Year **N+2**	Year **N+3**	… enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
TOTAL appropriations under HEADINGS 1 to 5	Commitments	**1.003**	**2.156**	**2.588**	**2.850**	**2.850**	**2.850**	**2.850**	**17.146**
	Payments	**1.003**	**2.156**	**2.588**	**2.850**	**2.850**	**2.850**	**2.850**	**17.146**

[57] Year N is the year in which implementation of the proposal/initiative starts.

of the multiannual financial framework									

3.1.1. Estimated impact on operational appropriations

6. ☐ The proposal/initiative does not require the use of operational appropriations

7. ☑ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to 3 decimal places)

Indicate objectives and outputs ⇩			Year **N=2014**		Year **N+1**		Year **N+2**		Year **N+3**		… enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
	Type of output[58]	Average cost of the output	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Total number of outputs	Total cost
SPECIFIC OBJECTIVE No 1			Consistency Mechanism															
- Output	Files[59]	0.050	5	0.250	10	0.500	10	0.500	8	0.400	8	0.400	8	0.400	8	0.400	57	2.850
Sub-total for specific objective N°1			**5**	**0.250**	**10**	**0.500**	**10**	**0.500**	**8**	**0.400**	**8**	**0.400**	**8**	**0.400**	**8**	**0.400**	**57**	**2.850**
SPECIFIC OBJECTIVE No 2			Implementing measures															
- Output	Cases[60]	0.250	0	0.000	1	0.150	2	0.300	3	0.450	3	0.450	3	0.450	3	0.450	15	2.250
Sub-total for specific objective N°2			**0**	**0.000**	**1**	**0.150**	**2**	**0.300**	**3**	**0.450**	**3**	**0.450**	**3**	**0.450**	**3**	**0.450**	**15**	**2.250**
SPECIFIC OBJECTIVE No 3			Adequacy of third countries															
Output	cases	0.200	2	0.400	4	0.800	4	0.800	4	0.800	4	0.800	4	0.800	4	0.800	26	5.200
Sub-total for specific objective N°3			**2**	**0.400**	**4**	**0.800**	**4**	**0.800**	**4**	**0.800**	**4**	**0.800**	**4**	**0.800**	**4**	**0.800**	**26**	**5.200**
TOTAL COST			**7**	**0.650**	**15**	**1.450**	**16**	**1.600**	**15**	**1.650**	**15**	**1.650**	**15**	**1.650**	**15**	**1.650**	**98**	**10.300**

58 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

59 Opinions, decisions, procedures meetings of the board.

60 Cases treated under the consistency mechanism

3.1.2. Estimated impact on appropriations of an administrative nature

3.1.2.1. Summary

8. ☐ The proposal/initiative does not require the use of administrative appropriations

9. ☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to 3 decimal places)

	Year N [61] 2014	Year N+1	Year N+2	Year N+3	… enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
HEADING 5 of the multiannual financial framework								
Human resources	0.318	0.636	0.890	1.081	1.081	1.081	1.081	**6.168**
Other administrative expenditure	0.035	0.070	0.098	0.119	0.119	0.119	0.119	0.678
Subtotal HEADING 5 of the multiannual financial framework	0.353	0.706	0.988	1.200	1.200	1.200	1.200	**6.846**

Outside HEADING 5 [62] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 5 of the multiannual financial framework								

TOTAL	0.353	0.706	0.988	1.200	1.200	1.200	1.200	**6.846**

61 Year N is the year in which implementation of the proposal/initiative starts.

62 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

3.1.2.1. Estimated requirements of human resources

10. ☐ The proposal/initiative does not require the use of human resources

11. ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	… enter as many years as necessary to show the duration of the impact (see point 1.6)		
• Establishment plan posts (officials and temporary agents)								
XX 01 01 01 (Headquarters and Commission's Representation Offices)		2	4	6	7	7	7	7
XX 01 01 02 (Delegations)								
• External personnel (in Full Time Equivalent unit: FTE)[63]								
XX 01 02 01 (CA, INT, SNE from the "global envelope")		1	2	2	3	3	3	3
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)								
XX 01 04 ***yy*** [64]	- at Headquarters[65]							
	- in delegations							
XX 01 05 02 (CA, INT, SNE - Indirect research)								
10 01 05 02 (CA, INT, SNE - Direct research)								
Other budget lines (specify)								
TOTAL		**3**	**6**	**8**	**10**	**10**	**10**	**10**

XX is the policy area or budget title concerned.

The additional staff is needed for the new tasks required in the consistency mechanism, for adequacy assessment of third countries and for the preparation of implementing measures. In total, an increase of 13 posts would be required for the new tasks related to the consistency mechanism (5 FTE), adequacy decisions (4 FTE) and implementing measures (4 FTE), which is partly offset by the staff freed from secretarial tasks for the Art 29 Working Party (3 FTE), as this task will be provided by the EDPS.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

63 CA= Contract Agent; INT= agency staff ("*Intérimaire*"); JED= "*Jeune Expert en Délégation*" (Young Experts in Delegations); LA= Local Agent; SNE= Seconded National Expert;

64 Under the ceiling for external personnel from operational appropriations (former "BA" lines).

65 Essentially for Structural Funds, European Agricultural Fund for Rural Development (EAFRD) and European Fisheries Fund (EFF).

Description of tasks to be carried out:

Officials and temporary agents	Case handlers, operating the data protection consistency mechanism to ensure unity of application of EU data protection rules. Tasks include investigation and research of cases submitted for decision from MS authorities, negotiation with MS and preparation of Commission decisions. Based on recent experience, 5 to 10 cases requiring invocation of the consistency mechanism may occur per year. The handling of adequacy requests requires the direct interaction with the requesting country, possibly the management of expert studies on the conditions at the country, assessment of the conditions, preparation of the relevant Commission decisions and of the process, including of the Committee assisting the Commission and any expert bodies as appropriate. Based on current experience, up to 4 adequacy requests can be expected per year. The process of adopting implementing measures includes preparatory measures, such as issue papers, research and public consultations, as well as the drafting of the actual instrument and management of the negotiation process in the relevant Committees and other groups, as well as stakeholder contacts in general. Across the areas requiring more precise guidance, up to three implementing measures may be handled per year, while the process may take up to 24 months, depending on the intensity of consultations.
External personnel	Administrative and secretarial support

3.1.3. Compatibility with the current multiannual financial framework

12. ☑ Proposal/initiative is compatible the current multiannual financial framework.

13. ☐ Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts.

14. ☐ Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[66].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.1.4. Third-party contributions

15. ☑The proposal/initiative does not provide for co-financing by third parties

16. The proposal/initiative provides for the co-financing estimated below:

Appropriations in EUR million (to 3 decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	… enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations cofinanced								

[66] See points 19 and 24 of the Interinstitutional Agreement.

3.2. Estimated impact on revenue

17. ☑ Proposal/initiative has no financial impact on revenue.

18. ☐ Proposal/initiative has the following financial impact:

- ☐ on own resources
- ☐ on miscellaneous revenue

EUR million (to 3 decimal places)

Budget revenue line:	Appropriations available for the ongoing budget year	Impact of the proposal/initiative[67]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	… insert as many columns as necessary in order to reflect the duration of the impact (see point 1.6)		
Article …….								

For miscellaneous assigned revenue, specify the budget expenditure line(s) affected.

Specify the method for calculating the impact on revenue.

[67] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25% for collection costs.

Annex to Legislative Financial Statement for proposal for a Regulation of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data.

Applied methodology and main underlying assumptions

The costs related to the new tasks to be carried out by the European Data Protection Supervisor (EDPS) stemming from the two proposals have been estimated for staff expenditure on the basis of the costs incurred by the Commission currently for similar tasks.

The EDPS will host the secretariat of the European Data Protection Board replacing the Article 29 Working Party. On the basis of the Commission current workload for this task, this results in the need for 3 additional FTE plus corresponding administrative and operational expenditure. This workload will have to be carried from the entry into force of the Regulation.

Furthermore, the EDPS will have a role in the consistency mechanism which is expected to require 5 posts, and in developing and operating a common IT tool for national DPAs, which will require 2 additional staff members.

The calculation of the increase in the required staff budget for the first seven years is presented in more detail in the table below. A second table shows the required operational budget. This will be reflected in the Budget of the EU in Section IX EDPS.

Cost type	Calculation	Amount (in thousands)						
		2014	2015	2016	2017	2018	2019	Total
Salaries and allowances								
- of EDPB Chair		0.300	0.300	0.300	0.300	0.300	0.300	1.800
- of which officials and temporary agents	=7*0.127	0.889	0.889	0.889	0.889	0.889	0.889	5.334
- of which SNEs	=1*0.073	0.073	0.073	0.073	0.073	0.073	0.073	0.438
- of which contract agents	=2*0.064	0.128	0.128	0.128	0.128	0.128	0.128	0.768
Expenditure related to recruitment	=10*0.005	0.025	0.025	0.013	0.013	0.013	0.013	0.100
Mission expenses		0.090	0.090	0.090	0.090	0.090	0.090	0.540
Other expenses, training	=10*0.005	0.050	0.050	0.050	0.050	0.050	0.050	0.300
Total Administrative expenditure		**1.555**	**1.555**	**1.543**	**1.543**	**1.543**	**1.543**	**9.280**

Description of tasks to be carried out:

Officials and temporary agents	Desk officers in charge of the secretariat of the Data Protection Board. Apart from logistics support, including budgetary and contractual issues, this includes the preparation of meeting agendas and expert invitations, research on subjects on the agenda of the group, management of the documents relating to the work of the group including the relevant data protection, confidentiality and public access requirements. Including all subgroups and expert groups, up to 50 meetings and decision procedures may have to be organised every year. Case handlers, operating the data protection consistency mechanism to ensure unity of application of EU data protection rules. Tasks include investigation and research of cases submitted for decision from MS authorities, negotiation with MS and preparation of Commission decisions. Based on recent experience, 5 to 10 cases requiring invocation of the consistency mechanism may occur per year. The IT tool shall simplify the operational interaction between national DPAs and data controllers obliged to share information with the public authorities. The responsible staff member(s) will ensure quality control, project management and budgetary follow-up of the IT processes on requirements engineering, implementation and operation of the systems.
External personnel	Administrative and secretarial support

Operational expenditure for EDPS

Indicate objectives and outputs			Year **N=2014**		Year **N+1**		Year **N+2**		Year **N+3**		enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
⇩	Type of output[68]	Average cost of the output	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Total number of outputs	Total cost
SPECIFIC OBJECTIVE No 1[69]			Secretariat to DP Board															
- Output	Cases[70]	0.010	30	0.300	40	0.400	50	0.500	50	0.500	50	0.500	50	0.500	50	0.500	320	3.200
Sub-total for specific objective N°1			30	0.300	40	0.400	50	0.500	50	0.500	50	0.500	50	0.500	50	0.500	320	3.200
SPECIFIC OBJECTIVE No 2			Consistency Mechanism															
- Output	Files[71]	0.050	5	0.250	10	0.500	10	0.500	10	0.500	8	0.400	8	0.400	8	0.400	59	2.950
Sub-total for specific objective N°2			5	0.250	10	0.500	10	0.500	10	0.500	8	0.400	8	0.400	8	0.400	59	2.950
SPECIFIC OBJECTIVE No 3			Common IT tool for DPAs (EDPS)															
- Output	Cases[72]	0.100	3	0.300	6	0.600	9	0.900	9	0.900	6	0.600	3	0.300	5	0.500	41	4.100
Sub-total for specific objective N°3			3	0.300	6	0.600	9	0.900	9	0.900	6	0.600	3	0.300	5	0.500	41	4.100
TOTAL COST			38	0.850	56	1.500	69	1.900	69	1.900	64	1.500	61	1.200	63	1.400	420	10.250

68 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

69 As described in Section 1.4.2. "Specific objective(s)…"

70 Cases treated under the consistency mechanism

71 Opinions, decisions, procedures meetings of the board.

72 The totals for each year estimate the efforts for developing and operating the IT tools