EUROPEAN
COMMISSION

Brussels, 10.1.2017
COM(2017) 8 final

2017/0002 (COD)

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 by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, establishes the principle that everyone has the right to the protection of personal data concerning them. Moreover, in Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal basis for adopting rules on the protection of personal data. Article 8 of the Charter of Fundamental Rights of the European Union enshrines the protection of personal data as a fundamental right.

The right to the protection of personal data also applies to the processing of personal data by EU institutions, bodies, offices and agencies. Regulation (EC) No 45/2001,[1] the main piece of existing EU legislation on personal data protection in the Union institutions, was adopted in 2001 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data throughout the Union. It was complemented by Decision No 1247/2002/EC.[2]

On 27 April 2016, the European Parliament and the Council adopted the General Data Protection Regulation (Regulation (EU) 2016/679), which will become applicable on 25 May 2018. This Regulation calls for Regulation (EC) No 45/2001 to be adapted to the principles and rules laid down in Regulation (EU) 2016/679 in order to provide a strong and coherent data protection framework in the Union and to enable both instruments to be applicable at the same time[3].

It is consistent with the coherent approach to personal data protection throughout the Union to align, as far as possible, the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the Member States. Whenever the provisions of the proposal are based on the same concept as the provisions of Regulation (EU) 2016/679, these two provisions should be interpreted homogeneously, in particular because the scheme of the proposal should be understood as the equivalent of the scheme of Regulation (EU) 2016/679.[4]

The review of Regulation (EC) No 45/2001 also takes into account the results of enquiries and stakeholder consultations, and the evaluation study on its application over the last 15 years.

This initiative is not within the Regulatory Fitness Programme (REFIT).

• Consistency with existing policy provisions in the policy area

The proposal aims to align the provisions of Regulation (EC) No 45/2001 with the principles and rules laid down in Regulation (EU) 2016/679 in order to provide a strong and coherent data protection framework in the Union. The proposal also incorporates the relevant rules laid down in Regulation (EC) XXXX/XX [e-Privacy Regulation] with regard to the protection of terminal equipment of end-users.

---

1 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 8, 12.1.2001.

2 Decision No 1247/2002/EC of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, OJ L 183, 12.07.2002, p. 1.

3 See Regulation (EU) 20016/679, Article 98 and recital 17.

4 See CJEU 9 March 2010, *Commission v Germany*, Case C-518/07, ECLI:EU:C:2010:125, paras 26 and 28.

- **Consistency with other Union policies**

Not applicable

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The protection of natural persons in relation to the processing of their personal data is a fundamental right laid down in Article 8(1) of the Charter of Fundamental Rights of the European Union.

This proposal is based on Article 16 TFEU, which is the legal basis for adopting data protection rules. This Article allows for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies when carrying out activities which fall within the scope of Union law. It also allows for the adoption of rules relating to the free movement of personal data, including personal data processed by those institutions, bodies, offices and agencies.

- **Subsidiarity (for non-exclusive competence)**

The subject- matter of this Regulation falls within the domain of exclusive competence of the Union, since only the Union can adopt rules governing the processing of personal data by the Union's institutions.

- **Proportionality**

In accordance with the principle of proportionality, to achieve the basic objectives of ensuring an equivalent level of protection of natural persons with regard to the processing of personal data and the free flow of personal data throughout the Union it is necessary and appropriate to lay down rules on processing personal data by Union institutions, bodies, offices and agencies. This Regulation does not go beyond what is necessary for achieving the objectives pursued in accordance with Article 5(4) of the Treaty on European Union.

- **Choice of the instrument**

A Regulation is considered the appropriate legal instrument to define the framework on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data. It provides natural persons with legally enforceable rights, specifies the data processing obligations of the controllers in the Union institutions, bodies, offices and agencies. It also provides for an independent supervisory authority, the European Data Protection Supervisor, to be responsible for monitoring the processing of personal data by the Union institutions, bodies, offices and agencies.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

The Commission carried out stakeholder consultations in 2010 and 2011 and an impact assessment in the context of preparing the data protection reform package which informs on the changes proposed to Regulation (EC) No 45/2001. In this context, the Commission also conducted a survey of Commission data protection coordinators (DPCs).[5]

---

[5] See at http://ec.europa.eu/justice/data-protection/reform/index_en.htm

As regards the practical application of Regulation (EC) No 45/2001 by Union institutions, bodies, offices and agencies, information was gathered from the European Data Protection Supervisor (EDPS), other Union institutions, bodies, offices and agencies, other Commission DG's and an external contractor. A questionnaire was send to the Network of data protection officers (DPOs).[6]

The data protection officers from a number of Union's institutions, bodies, offices and agencies held workshops on the reform of Regulation 45/2001 on 9 July 2015, 22 October 2015, 19 January 2016 and 15 March 2016.

The Commission decided in 2013 to conduct an evaluation study on the application to date of Regulation (EC) No 45/2001, which it outsourced to an external contractor. The final deliverables of the evaluation study (final report, five case studies and article-by-article analysis) were submitted to the Commission on 8 June 2015[7].

The evaluation showed that the governance system structured around DPOs and the EDPS is effective. It found that the sharing of powers between DPOs and the EDPS is clear and well balanced, and that both have an appropriate range of powers. Difficulties could, however, arise from a lack of authority due to insufficient support for the DPOs from their management.

The evaluation study indicated that Regulation (EC) No 45/2001 could be better enforced through the use of sanctions by the EDPS. Increased use of its supervisory authority powers could lead to better implementation of data protection rules. Another conclusion was that data controllers should adopt a risk management approach and perform risk assessments before carrying out processing operations in order to better implement data retention and security requirements.

The study also showed that existing rules in Chapter IV of Regulation (EC) No 45/2001 on the telecommunications sector are outdated and that there is a need to align this Chapter with the e-Privacy Directive. According to the evaluation study there is also a need to make some key definitions of Regulation (EC) No 45/2001 clearer. These include the identification of data controllers in the Union institutions, bodies, offices and agencies, the definition of recipients and extending the obligation on confidentiality to external processors.

The evaluation study also pointed to the need to simplify the regime of notifications and prior checks in order to increase efficiency and reduce the administrative burden.

The evaluator carried out an online survey in 64 Union institutions, agencies, offices and bodies. 422 responsible officials of data controllers, 73 DPOs, 118 DPCs and 109 IT respondents answered to the survey questions. The evaluator also carried out a series of stakeholder interviews. On 26 March 2015, the evaluator and the Commission organised a final workshop, attended by a number of data controllers, DPOs, DPCs, IT respondents and representatives of the EDPS.

- **Collection and use of expertise**

See reference to the evaluation study under the previous point.

---

6 See European Data Protection Supervisor's general report on 'Measuring compliance with Regulation (EC) 45/2001 in EU institutions ('Survey 2013')' and 'Opinion 3/2015 'Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform'.'

7 JUST/2013/FRAC/FW/0157/A4 in the context of the multiple framework contract JUST/2011/EVAL/01 (RS 2013/05) - Evaluation Study on Regulation (EC) 45/2001, by Ernst and Young, available on http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087

- **Impact assessment**

The impact of the present proposal will fall mainly on the Union institutions, bodies, offices and agencies. This has been confirmed by the information gathered from the EDPS, other Union institutions, bodies, offices and agencies, Commission DG's and the external contractor. Furthermore, the impact of the new obligations arising from Regulation (EU) 2016/679, with which the present regulation is to be aligned, has been assessed in the context of the preparatory works for the latter. This renders a specific impact assessment for this Regulation unnecessary.

- **Regulatory fitness and simplification**

Not applicable

- **Fundamental rights**

The right to the protection of personal data is laid down in Article 8 of the Charter of Fundamental Rights of the European Union (Charter), Article 16 of the TFEU and Article 8 of the European Convention on Human Rights. As underlined by the Court of Justice of the European Union,[8] the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.[9] Data protection is also closely linked to respect for private and family life protected by Article 7 of the Charter.

The present proposal lays down rules on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data.

Other fundamental rights enshrined in the Charter that could potentially be affected are: the freedom of expression (Article 11); the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination 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 of access to documents (Article 42); and the right to an effective remedy and a fair trial (Article 47*).*

4. BUDGETARY IMPLICATIONS

See the financial statement in annex.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Not applicable

- **Explanatory documents (for directives)**

Not applicable

CHAPTER I - GENERAL PROVISIONS

---

8 CJEU, 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09 ECLI:EU:C:2009:284, par. 48.

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

Article 1 defines the subject matter of the Regulation, and, as in Article 1 of Regulation (EC) No 45/2001, sets out the two objectives of the Regulation: protection of the fundamental right to data protection and to guarantee the free flow of personal data throughout the Union. It also provides for the main tasks of the European Data Protection Supervisor.

Article 2 determines the scope of the Regulation: it shall apply to the processing of personal data, by automated means or otherwise, by all Union institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Union law. The material scope of this Regulation is technologically neutral. The protection of personal data applies to the processing of personal data by automated means, as well as to manual processing if the personal data are contained or are intended to be contained in a filing system.

Article 3 contains definitions of terms used in the Regulation. Apart from the definitions of the 'Union institutions and bodies', 'controller', 'user' and 'directory', which are specific to this Regulation, the terms used in this Regulation are defined in Regulation (EU) 2016/679, Regulation (EU) 0000/00 [new ePrivacy Regulation], Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] and Commission Directive 2008/63/EC.

CHAPTER II - PRINCIPLES

Article 4 sets out the principles relating to personal data processing, which correspond to those in Article 5 of Regulation (EU) 2016/679. Compared to Regulation (EC) No 45/2001 it adds the new principles of transparency and of integrity and confidentiality.

Article 5 is based on Article 6 of Regulation (EU) 2016/679 and sets the criteria for lawful processing, with the sole exception of the criterion of the controller's legitimate interest which is not applicable to the public sector and thus should not apply to Unions institutions and bodies. Article 5 maintains the criteria already established under Article 5 of Regulation (EC) No 45/2001.

Article 6 clarifies the conditions for processing for another compatible purpose in line with Article 6(4) of Regulation (EU) 2016/679. Compared to Article 6 of Regulation (EC) No 45/2001 this new provision provides more flexibility and legal certainty with regard to further processing for compatible purposes.

Article 7 clarifies, in accordance with Article 7 of Regulation (EU) 2016/679, the conditions for consent to be valid as a legal ground for lawful processing.

Article 8 sets out, in line with Article 8 of Regulation (EU) 2016/679, further conditions for the lawfulness of the processing of personal data of children in relation to information society services offered directly to them. It sets 13 years as the child's minimum age for valid consent.

Article 9 sets out, in accordance with Article 8 of Regulation (EC) No 45/2001 rules providing for a specific level of protection on the transmission of personal data to recipients, other than Union institutions and bodies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680. It clarifies that, where it is the controller initiating the transmission, it should demonstrate necessity and proportionality of the transmission.

Article 10 sets out the general prohibition for processing special categories of personal data and the exceptions from this general rule, building on Article 9 of Regulation (EU) 2016/679 and further developing Article 10 of Regulation (EC) No 45/2001.

Article 11 sets out, in accordance with Article 10 of Regulation (EU) 2016/679 and in line with Article 10(5) of Regulation (EC) No 45/2001, the conditions for processing of personal data relating to criminal convictions and offences.

Article 12 clarifies the controller's information obligations towards the data subject, in accordance with Article 11 of Regulation (EU) 2016/679, providing that if the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.

Article 13 sets out, based on Article 89(1) of Regulation (EU) 2016/679, the rules on safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

CHAPTER III - RIGHTS OF THE DATA SUBJECT

Section 1 – Transparency and modalities

Article 14 introduces, based on Article 12 of of Regulation (EU) 2016/679, the obligation on controllers to provide transparent, easily accessible and understandable information and procedures and mechanism for exercising the data subject's rights, including where appropriate, means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals. As the Union institutions and bodies are not expected to charge, in any circumstance, fees related to the administrative costs for providing the information, this possibility was not taken over from Regulation (EU) 2016/679.

Section 2 – Information and access to data

Article 15 specifies the controller's information obligations towards the data subject where personal data are collected from the data subject, building on Article 13 of Regulation (EU) 2016/679 and further developing Article 11 of Regulation (EC) No 45/2001, providing information to the data subject, including on the storage period, the right to lodge a complaint and in relation to international transfers.

Article 16 further specifies, building on Article 14 of Regulation (EU) 2016/679 and further developing Article 12 of Regulation (EC) No 45/2001, the controller's information obligations towards the data subject where personal data have not been obtained from the data subject providing information to the source from which the data are originating. It also maintains the possible derogations in Regulation (EU) 2016/679, e.g. there will be no such obligation if the data subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort for the controller, where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law or if the recording or disclosure are expressly provided by law. This could apply for example in proceedings by services competent for social security or health matters.

Article 17 provides, in accordance with Article 15 of Regulation (EU) 2016/679 and further developing Article 13 of Regulation (EC) No 45/2001, on the data subject's right of access to their personal data, adding new elements, such as the obligation to inform the data subjects of the storage period, and of the rights to rectification and to erasure and to lodge a complaint.

Section 3 – Rectification and erasure

Article 18 sets out the data subject's right to rectification, based on Article 16 of Regulation (EU) 2016/679 and further developing Article 14 of Regulation (EC) No 45/2001.

Article 19 lays down, in accordance with Article 17 of Regulation (EU) 2016/679 and further developing Article 16 of Regulation (EC) No 45/2001, the data subject's right to be forgotten and to erasure. It provides the conditions of the right to be forgotten, including the obligation

of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data.

Article 20 introduces the right to have the processing restricted in certain cases, avoiding the ambiguous terminology "blocking" used in Regulation (EC) No 45/2001 and ensuring consistency with the new terminology under Article 18 of Regulation (EU) 2016/679.

Article 21 provides, in line with Article 19 of Regulation (EU) 2016/679 and further developing Article 17 of Regulation (EC) No 45/2001, for the controller's obligation to communicate to the recipients to whom the personal data have been disclosed any rectification or erasure of personal data or restriction unless it proves impossible or involves disproportionate effort. The controller shall also inform the data subject of those recipients if he or she requests it.

Article 22 introduces, in accordance with Article 20 of Regulation (EU) 2016/679, the data subject's right to data portability, i.e. the right to receive the personal data concerning him or her, which he or she has provided to a controller or to have such personal data transmitted directly to another controller, where technically feasible. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured, commonly used and machine-readable format. This right only applies where the processing is based on the data subject's consent or on a contract concluded by him or her.

Section 4 – Right to object and automated individual decision-making

Article 23 provides for the data subject's rights to object based on Article 21 of Regulation (EU) 2016/679 and further developing Article 18 of Regulation (EC) No 45/2001.

Article 24 concerns the data subject's right not to be subject to a measure based solely on automated processing including profiling in line with Article 22 of Regulation (EU) 2016/679 and further developing Article 19 of Regulation (EC) No 45/2001.

Section 5 – Restrictions

Article 25 allows for restrictions of the data subject's rights laid down in Articles 14 to 22 and in Articles 34 and 38 and of principles laid down in Article 4 (in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22). Such restrictions should be laid down in legal acts adopted on the basis of the Treaties or the internal rules of Union institutions and bodies. In case a possibility of such a restriction is not provided for in the legal acts adopted on the basis of the Treaties or the internal rules of Union institutions and bodies, the latter could impose an ad hoc restriction if it respects the essence of the fundamental rights and freedoms, in relation to a specific processing operation, and is a necessary and proportionate measure in a democratic society to safeguard one or more of the objectives allowing the restrictions on data subject rights. This approach is in line with Article 23 of Regulation (EU) 2016/679. However, by contrast to Article 23 of Regulation (EU) 2016/679 and in line with Article 20 of Regulation (EC) No 45/2001 the provision does not provide for the possibility to restrict the right to object and the right not to be subject to decisions based solely on automated processing. The requirements for restrictions are in line with the Charter of Fundamental Rights and the European Convention on Human Rights, as interpreted by the Court of Justice of the European Union and the European Court of Human Rights respectively.

CHAPTER IV - CONTROLLER AND PROCESSOR

Section 1 – General obligations

Article 26 builds on Article 24 of Regulation (EU) 2016/679 and introduces the "principle of accountability" by describing the obligation of responsibility of the controller to comply with this Regulation and to demonstrate compliance, including by way of adoption of appropriate technical and organisational measures and, where appropriate, internal policies and mechanisms for ensuring such compliance. Article 24(3) of Regulation (EU) 2016/679 was not kept in this provision as the Union institutions and bodies should not adhere to codes of conduct or certification mechanisms.

Article 27 sets out, in accordance with Article 25 of Regulation (EU) 2016/679, the obligations of the controller arising from the principles of data protection by design and by default.

Article 28 on joint controllers builds on Article 26 of Regulation (EU) 2016/679 to clarify the responsibilities of joint controllers - either Union institutions or bodies or not - as regards their internal relationship and towards the data subject. This provision rules on the situation where all joint controllers are covered by the same legal regime (this Regulation) and the situation where some are covered by this Regulation and some by another legal instrument (Regulation (EU) 2016/679, Directive (EU) 2016/680, Directive (EU) 2016/681 and other specific data protection regimes concerning Union institutions or bodies).

Article 29 builds on Article 28 of Regulation (EU) 2016/679 and further develops Article 23 of Regulation (EC) No 45/2001, to clarify the position and obligations of processors, including the determination that a processor who infringes the Regulation by determining the purposes and means of processing shall be considered to be a controller in respect of that processing.

Article 30 on the processing under the authority of the controller and processor is based on Article 29 of Regulation (EU) 2016/679, laying down a prohibition for the processor or any person acting under the authority of the controller or of the processor, and having access to personal data to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 31 builds on Article 30 of Regulation (EU) 2016/679, and introduces the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility, instead of a prior notification to the EDPS as required by Article 25 of Regulation (EC) No 45/2001 and the DPO register. By contrast to Regulation (EU) 2016/679, this provision does not make reference to representatives, as Unions institutions will not have representatives and will always have DPOs. References to transfers based on derogations for specific situations as in Regulation (EU) 2016/679 were not kept as those types of transfers are not envisaged in the present Regulation. The obligation to keep a record of processing activities may be centralised at the level of a Union institution or body. In such case, Union institutions and bodies have the possibility to keep their records of processing activities in the form of a publicly accessible register.

Article 32 clarifies, on the basis of Article 31 of Regulation (EU) 2016/679, the obligations of Union institutions and bodies for the co-operation with the EDPS.

Section 2 – Security of personal data and confidentiality of electronic communications

Article 33 obliges, in accordance with Article 32 of Regulation (EU) 2016/679 and further developing Article 22 of Regulation (EC) No 45/2001, the controller to implement appropriate measures for the security of processing extending that obligation to processors, irrespective of the contract with the controller.

Article 34 builds on Article 36 of Regulation (EC) No 45/2001 and ensures the confidentiality of electronic communications within Union institutions and bodies.

Article 35 builds on the existing practice of Union institutions and bodies and protects the information related to the terminal equipment of end-users who are accessing publicly available websites and mobile applications offered by Union institutions and bodies, in accordance with Regulation (EU) XXXX/XX [new ePrivacy Regulation], in particular Article 8 thereof.

Article 36 is based on Article 38 of Regulation (EC) No 45/2001 and protects personal data held in public and private directories of Union institutions and bodies.

Articles 37 and 38 introduce an obligation to notify personal data breaches, in accordance with Articles 33 and 34 Regulation (EU) 2016/679.

Section 3 – Data protection impact assessment and prior consultation

Article 39 builds on Article 35 of Regulation (EU) 2016/679 and introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to processing operations which are likely to result in a high risk to the rights and freedoms of natural persons. This obligation will apply in particular in case of systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, processing on a large scale of special categories of data or systematic monitoring of a publicly accessible area on a large scale.

Article 40 is based on Article 36 of Regulation (EU) 2016/679 and concerns the cases where authorisation by, and consultation of, the EDPS is mandatory prior to the processing. However, the first paragraph of Article 40 reproduces recital 94 of Regulation (EU) 2016/679 and is aimed at clarifying the scope of the obligation to consult.

Section 4 – Information and legislative consultation

Article 41 provides for an obligation for Union institutions and bodies to inform the EDPS when drawing up administrative measures and internal rules relating to the processing of personal data.

Article 42 provides for an obligation for the Commission to consult the EDPS following the adoption of proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts that have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. Where those acts have a particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases both entities should coordinate their work with a view to issue a joint opinion. A time limit of 8 weeks for the issue of the advice in aforementioned cases is established, with possible derogations for urgent cases and otherwise where appropriate, for example when the Commission is preparing delegated and implementing acts.

Section 5 – Obligation to react to allegations

Article 43 lays down the obligation of controllers and processor to react to allegations after the EDPS decided to refer a matter to them.

Section 6 – Data protection officer

Article 44 builds on Article 37 (1) (a) Regulation (EU) 2016/679 and Article 24 of Regulation (EC) No 45/2001 to provide a mandatory DPO for Unions institutions and bodies.

Article 45 builds on 38 of Regulation (EU) 2016/679 and Article 24 of Regulation (EC) No 45/2001 to set out the position of the DPO.

Article 46 builds on 39 of Regulation (EU) 2016/679 and Article 24 and on the second and third paragraphs of the Annex to Regulation (EC) No 45/2001 to provide the core tasks of the DPO.

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

Article 47 further builds on Article 9 of Regulation (EC) No 45/2001 and spells out the general principle, in accordance with Article 44 of Regulation (EU) 2016/679, that compliance with other provisions of this Regulation and the conditions laid down in Chapter V are mandatory for any transfers of personal data to third countries or international organisations, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

Article 48 sets that a transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that an adequate level of protection is ensured in the third country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out. Paragraphs 2 and 3 of this Article have been taken over from Article 9 of Regulation (EC) No 45/2001 as they are useful elements for monitoring of the level of protection in third countries and international organisations.

Article 49 builds on Article 46 of Regulation (EU) 2016/679 and 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 and contractual clauses. Binding corporate rules, codes of conduct and certification mechanisms could be used, in accordance with Regulation (EU) 2016/679, by processors other than Union institutions and bodies. The fourth paragraph of this Article on the obligation of Union institutions and bodies to inform the EDPS of categories of cases where they have applied this Article corresponds to Article 9(8) of Regulation (EC) No 45/2001 and is kept due to its specificity. The fifth paragraph builds on the grandfathering of existing authorisations laid down in Article 46(5) of Regulation (EU) 2016/679.

Article 50 clarifies in accordance with Article 48 of Regulation (EU) 2016/679, that judgment of courts or decisions of administrative authorities of third countries requiring a transfer or disclosure of personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 51 builds on Article 49 of Regulation (EU) 2016/679 and spells out and clarifies the derogations for a data transfer. This applies in particular to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers involving competition authorities, tax or customs administrations, or between services competent for social security matters or for fisheries management. The fifth paragraph on the obligation to inform the EDPS of categories of cases where derogations have been relied upon for a transfer corresponds to the current Article 9(8) of Regulation (EC) No 45/2001.

Article 52 is based on Article 50 Regulation (EU) 2016/679 and explicitly provides for international co-operation mechanisms for the protection of personal data between the EDPS, in cooperation with the Commission and the European Data Protection Board, and the supervisory authorities of third countries.

CHAPTER VI - THE EUROPEAN DATA PROTECTION SUPERVISOR

Article 53 builds up on Article 41 of Regulation (EC) No 45/2001 and concerns the establishment of the EDPS.

Article 54 builds on Article 42 of Regulation (EC) No 45/2001 and on Article 3 of Decision 1247/2002/EC and sets out the rules for the appointment of the EDPS by the European Parliament and the Council. It also specifies the duration of its term of office: five years.

Article 55 builds on Article 43 of Regulation (EC) No 45/2001 and on Article 1 of Decision 1247/2002/EC and provides for regulations and general conditions governing the performance of duties of the EDPS and his or her staff and the financial resources.

Article 56 builds on Article 52 Regulation (EU) 2016/679 and Article 44 of Regulation (EC) No 45/2001 and clarifies the conditions for the independence of the EDPS, taking into account the case law of the Court of Justice of the European Union.

Article 57 sets, based on Article 45 of Regulation (EC) No 45/2001, the duties of secrecy of the EDPS during and after the term of office with regard to confidential information which has come to his or her knowledge in the course of the performance of the official duties.

Article 58 builds on Article 57 Regulation (EU) 2016/679 and Article 46 of Regulation (EC) No 45/2001 and sets the tasks of the EDPS, including hearing and investigating complaints and promoting the awareness of the public of risks, rules, safeguards and rights.

Article 59 is based on Article 58 of Regulation (EU) 2016/679 and Article 47 of Regulation (EC) No 45/2001 and sets out the powers of the EDPS.

Article 60 builds on Article 59 of Regulation (EU) 2016/679 and Article 48 Regulation (EC) 45/2001 and lays down the obligation for the EDPS to draw up an annual activity report.

CHAPTER VII - COOPERATION AND CONSISTENCY

Article 61 builds on Article 61 Regulation (EU) 2016/679 and Article 46(f) of Regulation (EC) No 45/2001 and introduces explicit rules on cooperation of EDPS with national supervisory authorities.

Article 62 provides for the obligations of the EDPS where other Union acts refer to this Article in the framework of coordinated supervision with national supervisory authorities. It seeks to implement a single model of coordinated supervision. This model could be used for coordinated supervision of large IT systems such as Eurodac, Schengen Information System II, Visa Information System, Customs Information System or Internal Market Information System, but also for supervision of some Union agencies where a specific model of cooperation between EDPS and national authorities is established, such as Europol. The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the board.

CHAPTER VIII - REMEDIES, LIABILITY AND PENALTIES

Article 63 is based on Article 77 of Regulation (EU) 2016/679 and Article 32 of Regulation (EC) No 45/2001 and provides the right of any data subject to lodge a complaint with the EDPS. It lays down also the obligation of the EDPS to handle and inform the data subject of the progress and the outcome of the complaint within a deadline of three months after which the complaint shall be deemed to have been rejected.

Article 64 maintains Article 32 (1) of Regulation (EC) No 45/2001, setting out the jurisdiction of the Court of Justice of the European Union to hear all disputes which relate to the provisions of this Regulation, including claims for damages.

Article 65 sets out the right to compensation, for both material and non-material damage, subject to the conditions, including on liability, provided for in the Treaties.

Article 66 builds on Article 83 of Regulation (EU) 2016/679 and provides the EDPS with the power to impose administrative fines on Union institutions and bodies, as a sanction of last resort and only where Union institution or bodies failed to comply with an order by the EDPS referred to in Article 59(2)(a) to (h) and (j). The article also specifies the criteria for deciding on the amount of the administrative fine in each individual case, while the maximum yearly ceilings are inspired by amounts of fines applicable in some Member States.

Article 67 allows, in accordance with Article 80(1) of Regulation (EU) 2016/679, certain bodies, organisations or associations to lodge a complaint on behalf of the data subject.

Article 68 provides, in line with Article 33 of Regulation (EC) No 45/2001, for specific rules aimed at protecting Union's staff, which lodge a complaint with the EDPS regarding an alleged infringement of the provisions of this Regulation, without acting through official channels.

Article 69 builds on Article 49 of Regulation (EC) No 45/2001 and provides on sanctions applicable to failures to comply with the obligations of this Regulation by officials or other civil servants of the European Union.

CHAPTER IX - IMPLEMENTING ACTS

Article 70 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.

CHAPTER X - FINAL PROVISIONS

Article 71 repeals Regulation (EC) No 45/2001 and Decision No 1247/2002/EC and provides that references to the two repealed instruments are to be read as references to the present Regulation.

Article 72 clarifies that the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation. and that Articles 54(4), (5) and (7), and Articles 56 and 57 of the Regulation apply to the current Assistant Supervisor until the end of his term, i.e. until 5 December 2019.

Article 73 sets out 25 May 2018 as the date of entry into force of this Regulation in order to ensure consistency with the date of application of Regulation (EU) 2016/679.

2017/0002 (COD)

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 by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

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,

Having regard to the opinion of the European Economic and Social Committee[10],

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 (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning them.

(2) Regulation (EC) No 45/2001 of the European Parliament and of the Council[11] provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.

(3) Regulation (EU) 2016/679 of the European Parliament and of the Council[12] and Directive (EU) 2016/680 of the European Parliament and of the Council[13] were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.

(4) Regulation (EU) 2016/679 stresses the need for the necessary adaptations of Regulation (EC) No 45/2001 in order to provide a strong and coherent data protection framework in the Union and to allow application at the same time as Regulation (EU) 2016/679.

(5) It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions and bodies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation are based on the same concept as the provisions of

---

10 OJ C , , p. .

11 Regulation (EC) No 45/2001 of the European Parliament and 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 8, 12.1.2001, p.1).

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

13 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

Regulation (EU) 2016/679, those two provisions should be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.

(6) Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(7) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal 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.

(8) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. This Regulation should therefore apply to Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation only to the extent that Union law applicable to such agencies does not contain specific rules on the processing of personal data.

(9) Directive (EU) 2016/680 provides harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to foster the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union agencies carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation and competent authorities in Member States, the rules for the protection and the free movement of operational personal data processed by such Union agencies should draw on the principles underpinning this Regulation and be consistent with Directive (EU) 2016/680.

(10) Where the founding act of a Union agency carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of the Treaty lays down a standalone data protection regime for the processing of operational personal data such regimes should be unaffected by this Regulation. However, the Commission should, in accordance with Article 62 of Directive (EU) 2016/680, by 6 May 2019 review Union acts which regulate processing by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and, where appropriate, make the necessary proposals to amend those

acts to ensure a consistent approach to the protection of personal data in the area of judicial cooperation in criminal matters and police cooperation.

(11) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(12) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(13) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(14) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(15) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in

respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(16) In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within or to other Union institutions or bodies, they should verify whether such personal data is required for the legitimate performance of tasks covered by the competence of the recipient where the recipient is not part of the controller. In particular, following a recipient's request for transmission of personal data, the controller should verify the existence of a relevant ground of its lawful processing of personal data, the competence of the recipient and should make a provisional evaluation of the necessity for the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity for the transmission of the data can be subsequently verified.

(17) In order for processing to be lawful, personal data should be processed on the basis of the necessity of performance of a task carried out in the public interest by Union institutions and bodies or in the exercise of their official authority, the necessity for compliance with the legal obligation to which the controller is subject or some other legitimate basis as referred to in this Regulation, including the consent of the data subject concerned or the necessity 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. Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(18) The Union law including the internal rules referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in

accordance with the case-law of the Court of Justice of the European Union and the European Court of Human Rights.

(19) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

(20) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given 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 of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[14] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(21) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to creating personality profiles and the collection of personal data with regard to children when using services offered directly to a child on websites of Union institutions and bodies, such as interpersonal communication services or online selling of tickets and when the processing of personal data is based on consent.

(22) When recipients established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680, would like to have personal data transmitted to them by Union institutions and bodies, those recipients should demonstrate that the transmission is necessary for the attainment of their objective, is proportionate and does not go beyond what is necessary to attain that objective. Union institutions and

---

[14] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ J 95, 21.4.1993, p.29).

bodies should demonstrate such necessity when they themselves initiate the transmission, in compliance with the principle of transparency.

(23) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or 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.

(24) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[15], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties.

(25) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(26) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or

---

[15] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, which may include internal rules.

(27) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(28) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(29) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(30) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic

personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(31) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(32) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(33) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(34) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should therefore not

apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(35) Where personal data might lawfully be processed because 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, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(36) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union law. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(37) Legal acts adopted on the basis of the Treaties or internal rules of Union institutions and bodies may impose restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, confidentiality of electronic communications as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, including the protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes.

Where a restriction is not provided for in legal acts adopted on the basis of the Treaties or their internal rules, Union institutions and bodies may in a specific case impose an ad hoc restriction concerning specific principles and the rights of data subject if such a restriction respects the essence of the fundamental rights and freedoms and, in relation to a specific processing operation, is necessary and proportionate in a democratic society to safeguard one or more of the objectives mentioned in paragraph 1. The restriction should be notified to the data protection officer. All restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(38) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective

assessment, by which it is established whether data processing operations involve a risk or a high risk.

(39) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

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

(41) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.

(42) In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records, on request, available to it, so that they might serve for monitoring those processing operations. Union institutions and bodies should be able to establish a central register of records of their processing activities. For reasons of transparency, they should also be able to make such a register public.

(43) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(44) Union institutions and bodies should ensure the confidentiality of electronic communications as provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communication networks, protect the information related to end-users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XXXX/XX [new ePrivacy Regulation] and protect the personal data in directories of users.

(45) A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the European Data Protection Supervisor without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.

(46) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the European Data Protection Supervisor, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.

(47) Regulation (EC) No 45/2001 provides for a general obligation of the controller to notify the processing of personal data to the data protection officer, who would in turn keep a register of processing operations notified. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations could be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where

they become necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(48) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person. The European Data Protection Supervisor should respond to the request for consultation within a specified period. However, the absence of a reaction of the European Data Protection Supervisor within that period should be without prejudice to any intervention of the European Data Protection Supervisor in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, it should be possible to submit the outcome of a data protection impact assessment carried out with regard to the processing at issue to the European Data Protection Supervisor, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(49) The European Data Protection Supervisor should be informed about administrative measures and internal rules of Union institutions and bodies which provide for the processing of personal data, lay down conditions for restrictions of data subject rights or provide appropriate safeguards for data subject rights, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(50) Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise its supervisory and advisory functions in respect of all Union institutions and bodies, including on its own initiative or upon request. In order to ensure consistency of data protection rules throughout the Union, a consultation by the Commission should be obligatory following the adoption of legislative acts or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and following the adoption of recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU, which have an impact on the right to personal data protection. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except when the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification mechanisms. Where the act in question is of particular importance for the protection of individuals' rights and

freedoms with regard to the processing of personal data, the Commission should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate its work with the latter with a view to issue a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide its written advice within eight weeks. That time-frame should be shorter in case of urgency or otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.

(51) In each Union institution or body a data protection officer should ensure that the provisions of this Regulation are applied and should advise controllers and processors on fulfilling their obligations. That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers should be in a position to perform their duties and tasks in an independent manner.

(52) When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(53) The Commission can decide, under Article 45 of Regulation (EU) 2016/679, that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.

(54) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of making use of standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the European Data Protection Supervisor or contractual clauses authorised by the European Data Protection Supervisor. Where the processor is not a Union Institution or body those appropriate safeguards can also consist of binding corporate rules, codes of conduct and certification mechanisms used for international transfers under Regulation (EU) 2016/679. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by Union institutions and bodies to public authorities or bodies in third countries or to international organisations with corresponding duties or functions, including on the basis of provisions to be inserted

into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the European Data Protection Supervisor should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(55) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by the European Data Protection Supervisor should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by the European Data Protection Supervisor or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard data-protection clauses.

(56) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law.

(57) Provision should be made in specific situations for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union law so require 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. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by Union law, 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, taking into full account the interests and fundamental rights of the data subject.

(58) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between Union institutions and bodies and competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law may, for important

reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(59) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(60) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities in the Union, including the European Data Protection Supervisor, can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction. Their efforts to work together in the cross-border context can also be hampered by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, closer cooperation between the European Data Protection Supervisor and other data protection supervisory authorities should be promoted to help the exchange of information with their international counterparts.

(61) The establishment of the European Data Protection Supervisor in Regulation (EC) No 45/2001, empowered to perform its tasks and exercise its powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify its role and independence.

(62) In order to ensure consistent monitoring and enforcement of data protection rules throughout the Union, the European Data Protection Supervisor should have the same tasks and effective powers as the supervisory authorities in Member States, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and to bring infringements of this Regulation to the attention of the Court of Justice of the European Union and engage in legal proceedings in accordance with the primary law. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. In order to avoid superfluous costs and excessive inconveniencies for the persons concerned who might be adversely affected, each measure of the European Data Protection Supervisor should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, should take into account the circumstances of each individual case and respect the right of every person to be heard before taking any individual measure. Each legally binding measure of the European Data Protection Supervisor should be in writing, be clear and unambiguous, indicate the date of issue of the measure, bear the signature of the European Data Protection Supervisor, give the reasons for the measure, and refer to the right of an effective remedy.

(63) The decisions of the European Data Protection Supervisor regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently

of the publication of an annual activities report, the European Data Protection Supervisor can publish reports on specific subjects.

(64) The national supervisory authorities monitor the application of Regulation (EU) 2016/679 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. In order to increase the consistency in application of data protection rules applicable in Member States and data protection rules applicable to Union institutions and bodies, the European Data Protection Supervisor should effectively cooperate with the national supervisory authorities.

(65) In certain instances, Union law provides for a model of coordinated supervision, shared between the European Data Protection Supervisor and the national supervisory authorities. Moreover, the European Data Protection Supervisor is the supervisory authority of Europol and a specific model of cooperation with the national supervisory authorities is established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, a single, coherent model of coordinated supervision should be introduced in the Union. The Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation. The European Data Protection Board should serve as a single forum for ensuring the effective coordinated supervision across the board.

(66) Every data subject should have the right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice of the European Union in accordance with the Treaties, if the data subject considers that his or her rights under this Regulation are infringed or where the European Data Protection Supervisor does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The European Data Protection Supervisor should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further coordination with a national supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, the European Data Protection Supervisor should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(67) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation should have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaty.

(68) In order to strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the institution or body – rather than individuals – for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies. This Regulation should indicate infringements and the upper limits and criteria for setting the related administrative fines. The European

Data Protection Supervisor should determine the amount of fines in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. When imposing an administrative fine on a Union body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice of the European Union.

(69) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with the European Data Protection Supervisor. Such a body, organisation or association should also be able to exercise the right to a judicial remedy on behalf of data subjects or exercise the right to receive compensation on behalf of data subjects.

(70) An official or other servant of the Union who fails to comply with the obligations in this Regulation should be liable to disciplinary or any other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.

(71) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council[16]. The examination procedure should be used for the adoption of standard contractual clauses between controllers and processors and between processors, for the adoption of list of processing operations where prior consultation of the European Data Protection Supervisor is required by controllers processing for the performance of a task carried out in the public interest, and for the adoption of standard contractual clauses providing appropriate safeguards for international transfers.

(72) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU. Regulation (EC) No 223/2009 of the European Parliament and of the Council[17] provides further specifications on statistical confidentiality for European statistics.

---

16 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).

17 Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(73) Regulation (EC) No 45/2001 and Decision No 1247/2002/EC should be repealed. The references to the repealed Regulation and the Decision should be construed as references to this Regulation.

(74) In order to safeguard the full independence of the members of the independent supervisory authority, the terms of office of the current European Data Protection Supervisor and the current Assistant Supervisor should not be affected by this Regulation. The current Assistant Supervisor should remain in place until the end of his term of office, unless one of the conditions for the premature end of term of the European Data Protection Supervisor laid down in this Regulation is met. The relevant provisions of this Regulation should apply to the Assistant Supervisor until the end of his term of office.

(75) In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of ensuring an equivalent level of protection of natural persons and the free flow of personal data throughout the Union to lay down rules on processing of personal data in Union institutions and bodies. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with Article 5(4) of the Treaty on European Union.

(76) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on XX/XX/XXXX.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1
Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and rules relating to the free movement of personal data between themselves or to recipients established in the Union and subject to Regulation (EU) 2016/679[18] or the provisions of national law adopted pursuant to Directive (EU) 2016/680[19].

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The European Data Protection Supervisor ('EDPS') shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Union institution or body.

---

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

[19] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

Article 2
Scope

1. This Regulation applies to the processing of personal data by all Union institutions and bodies insofar as such processing is carried out in the exercise of activities which fall, wholly or partially within the scope of Union law.

2. This Regulation shall apply to the processing of personal data, wholly or partially by automated means, and to the processing otherwise than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 3
Definitions

1. For the purposes of this Regulation, the following definitions shall apply:

   (a) the definitions in Regulation (EU) 2016/679, with the exception of the definition of 'controller' in point (7) of Article 4 of that Regulation;

   (b) the definition of 'electronic communication' in point (a) of Article 4(2) of Regulation (EU) XX/XXXX [ePrivacy Regulation];

   (c) the definitions of 'electronic communication network' and 'end-user' in points (1) and (14) of Article 2 of Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] respectively;

   (d) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC[20].

2. In addition, for the purposes of this Regulation the following definitions shall apply:

   (a) 'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the Functioning of the European Union or the Euroatom Treaty;

   (b) 'controller' means the Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.

   (c) 'user' means any natural person using a network or terminal equipment operated under the control of a Union institution or body;

   (d) 'directory' means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.

---

[20] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162 21.06.2008 p. 20).

CHAPTER II

PRINCIPLES

Article 4
Principles relating to processing of personal data

1. Personal data must be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes (‘purpose limitation’);

   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay (‘accuracy’);

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

   (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 5
Lawfulness of processing

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

   (a) processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority vested in the Union institution or body;

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

(c) 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;

(d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

2. The tasks referred to in point (a) of paragraph 1 shall be laid down in Union law.

Article 6
Processing for another compatible purpose

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7
Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

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. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a

service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to children's consent in relation to information society services

1. Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Transmissions of personal data to recipients, other than Union institutions and bodies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680

1. Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transmitted to recipients established in the Union and subject to Regulation (EU) 2016/679 or to the national law adopted pursuant to Directive (EU) 2016/680, if the recipient establishes:

   (a) that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of official authority, or

   (b) that it is necessary to have the data transmitted, it is proportionate to the purposes of the transmission and if there is no reason to assume that the data subject's rights and freedoms and legitimate interests might be prejudiced.

2. Where the transmission under this Article takes place on the initiative of the controller, the controller shall demonstrate that the transmission of personal data is necessary and proportionate to the purposes of the transmission, by applying the criteria laid down in points (a) or (b) of paragraph 1.

Article 10

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   (a) the data subject has given explicit consent to the processing of those data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject, or

(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 non-profit-seeking body which constitutes an entity integrated in a Union institution or body and 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 this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects;

(e) 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 or whenever the Court of Justice of the European Union is acting in its judicial capacity, or

(g) processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union law.

Article 11

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 5(1) may be carried out only if authorised by Union law, which may include internal rules, providing the appropriate specific safeguards for the rights and freedoms of data subjects.

Article 12

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 13

Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

SECTION 1

TRANSPARENCY AND MODALITIES

Article 14

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any communication under Articles 17 to 24 and 38 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information

addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.

5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. If the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.

SECTION 2

INFORMATION AND ACCESS TO PERSONAL DATA

Article 15

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

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

   (a) the identity and the contact details of the controller;

   (b) the contact details of the data protection officer;

   (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

   (d) the recipients or categories of recipients of the personal data, if any;

   (e) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

   (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

   (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

   (c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

   (d) the right to lodge a complaint with the European Data Protection Supervisor;

   (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

   (f) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 16

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

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

   (a) the identity and the contact details of the controller;

   (b) the contact details of the data protection officer;

   (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

   (d) the categories of personal data concerned;

   (e) the recipients or categories of recipients of the personal data, if any;

   (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:

   (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

   (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

   (c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

   (d) the right to lodge a complaint with the European Data Protection Supervisor;

   (e) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

   (f) the existence of automated decision-making, including profiling, referred to in Article 24 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2;

   (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

   (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

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

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;

(c) obtaining or disclosure is expressly laid down by Union law; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law.

Article 17
Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

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

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

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

(f) the right to lodge a complaint with the European Data Protection Supervisor;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 49 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

SECTION 3

RECTIFICATION AND ERASURE

Article 18
Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 19
Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

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

   (b) the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 10(2), and where there is no other legal ground for the processing;

   (c) the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;

   (d) the personal data have been unlawfully processed;

   (e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject;

   (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

   (a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 10(2) as well as Article 10(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 20
Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

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

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

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

4. In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.

Article 21
Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 18, Article 19(1) and Article 20 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 22
Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 10(2) or on a contract pursuant to point (c) of Article 5(1); and

   (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

SECTION 4

RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Article 23
Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

3. Without prejudice to Articles 34 and 35, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using technical specifications.

4. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 24
Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

   (a) is necessary for entering into, or performance of, a contract between the data subject and the controller;

   (b) is authorised by Union law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

SECTION 5

RESTRICTIONS

Article 25
Restrictions

1. Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

   (a) the national security, public security or defence of the Member States;

   (b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

   (c) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

   (d) the internal security of Union institutions and bodies, including of their electronic communication networks;

   (e) the protection of judicial independence and judicial proceedings;

(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c).

(h) the protection of the data subject or the rights and freedoms of others;

(i) the enforcement of civil law claims.

2. Where a restriction is not provided for by a legal act adopted on the basis of the Treaties or by an internal rule in accordance with paragraph 1, the Union institutions and bodies may restrict the application of Articles 14 to 22, 34 and 38, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, if such a restriction respects the essence of the fundamental rights and freedoms, in relation to a specific processing operation, and is a necessary and proportionate measure in a democratic society to safeguard one or more of the objectives referred to in paragraph 1. The restriction shall be notified to the competent data protection officer.

3. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal rules, may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where personal data are processed for archiving purposes in the public interest, Union law, which may include internal rules, may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

5. Internal rules referred to in paragraphs 1, 3 and 4 shall be sufficiently clear and precise and subject to appropriate publication.

6. If a restriction is imposed pursuant to paragraphs 1 or 2, the data subject shall be informed, in accordance with Union law, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the European Data Protection Supervisor.

7. If a restriction imposed pursuant to paragraphs 1 or 2 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

8. Provision of the information referred to in paragraphs 6 and 7 and in Article 46(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 or 2.

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1

GENERAL OBLIGATIONS

Article 26
Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

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

Article 27
Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, 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, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 28
Joint controllers

1. Where a Union institution or body together with one or more controllers, which may be Union institutions or bodies or not, jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by

means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. The data subject may exercise his or her rights under this Regulation in respect of and against one or more of the joint controllers, taking into account their roles as determined in the terms of the arrangement referred to in paragraph 1.

Article 29
Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

   (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) takes all measures required pursuant to Article 33;

   (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

   (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, 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) assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 40 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. When a processor is not a Union institution or body, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than a Union institution or body pursuant to Article 42 of Regulation (EU) 2016/679.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 70(2).

8. The European Data Protection Supervisor may adopt standard contractual clauses for the matters referred to in paragraphs 3 and 4.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 30
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 those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 31
Records of processing activities

1. Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
   (a) the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;
   (b) the purposes of the processing;
   (c) a description of the categories of data subjects and of the categories of personal data;
   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organisations;
   (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
   (f) where possible, the envisaged time limits for erasure of the different categories of data;
   (g) where possible, a general description of the technical and organisational security measures referred to in Article 33.
2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
   (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;
   (b) the categories of processing carried out on behalf of each controller;
   (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
   (d) where possible, a general description of the technical and organisational security measures referred to in Article 33.
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. Union institutions and bodies shall make the record available to the European Data Protection Supervisor on request.
5. Union institutions and bodies may decide to keep their records of processing activities in a central register. In this case, they may also decide to make the register publicly accessible.

Article 32
Co-operation with the European Data Protection Supervisor

Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.

SECTION 2

SECURITY OF PERSONAL DATA AND CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS

Article 33
Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   (a) the pseudonymisation and encryption of personal data;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.

Article 34
Confidentiality of electronic communications

Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communication networks.

Article 35
Protection of information related to end-users' terminal equipment

Union institutions and bodies shall protect the information related to end–users' terminal equipment accessing their publicly available websites and mobile applications in accordance with Regulation (EU) XX/XXXX [new ePrivacy Regulation], in particular Article 8 thereof.

Article 36
Directories of users

1. Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

2. Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for direct marketing purposes.

Article 37
Notification of a personal data breach to the European Data Protection Supervisor

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

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

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

   (b) communicate the name and contact details of the data protection officer;

   (c) describe the likely consequences of the personal data breach;

   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall inform the data protection officer about the personal data breach.

6. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article.

Article 38
Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 37(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

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

   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 39
Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   (b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or

   (c) a systematic monitoring of a publicly accessible area on a large scale.

4. The European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

6. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including 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.

7. Compliance with approved codes of conduct referred to in Article 40 of the Regulation (EU) 2016/679 by the relevant processors other than Union institutions and bodies shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.

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

9. Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 shall not apply unless the Union law provides otherwise.

10. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 40
Prior consultation

1. The controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation. The controller shall seek the advice of the data protection officer about the need for prior consultation.

2. Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall, within period of up to eight weeks of receipt of the

request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 59. That period may be extended by six weeks, taking into account the complexity of the intended processing. The European Data Protection Supervisor shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the European Data Protection Supervisor has obtained information it has requested for the purposes of the consultation.

3. When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:

   (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;

   (b) the purposes and means of the intended processing;

   (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

   (d) the contact details of the data protection officer;

   (e) the data protection impact assessment provided for in Article 39; and

   (f) any other information requested by the European Data Protection Supervisor.

4. The Commission may, by means of implementing act, determine a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.

SECTION 4

INFORMATION AND LEGISLATIVE CONSULTATION

Article 41
Information

The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data involving a Union institution or body alone or jointly with others.

Article 42
Legislative consultation

1. Following the adoption of proposals for a legislative act and of recommendations or proposals to the Council pursuant to Article 218 TFEU and when preparing delegated acts or implementing acts, which have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.

2. Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases

the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issue a joint opinion.

3. The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or otherwise appropriate, the Commission may shorten the deadline.

4. This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.

SECTION 5

OBLIGATION TO REACT TO ALLEGATIONS

Article 43
Obligation to react to allegations

Where the European Data Protection Supervisor exercises the powers provided for in points (a), (b) and (c) of Article 59(2), the controller or processor concerned shall inform the European Data Protection Supervisor of its views within a reasonable period to be specified by the European Data Protection Supervisor, taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.

SECTION 6

DATA PROTECTION OFFICER

Article 44
Designation of the data protection officer

1. Each Union institution or body shall designate a data protection officer.

2. Union institutions and bodies may designate a single data protection officer for several of them, taking into account their organisational structure and size.

3. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 46.

4. The data protection officer may be a staff member of the Union institution or body, or fulfil the tasks on the basis of a service contract.

5. The Union institutions and bodies shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.

Article 45
Position of the data protection officer

1. The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 46 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The Union institutions and bodies shall ensure that the data protection officer does not receive any instructions regarding the exercise of his or her tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

7. The data protection officer may be consulted by the controller and the processor, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the competent data protection officer alleging that a breach of the provisions of this Regulation has taken place.

8. The data protection officer shall be designated for a term of three to five years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.

9. After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or body which designated him or her.

Article 46
Tasks of the data protection officer

1. The data protection officer shall have the following tasks:

   (a) inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;

   (b) ensure in an independent manner the internal application of this Regulation and to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;

(c) ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;

(d) provide advice where requested as regards the necessity for a notification or a communication of personal data breach pursuant to Articles 37 and 38;

(e) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment;

(f) provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 and to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;

(g) respond to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative.

2. The data protection officer may make recommendations for the practical improvement of data protection to the controller and the processor and advise them on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the controller or the processor, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.

3. Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 47
General principle 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 shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 48
Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that an adequate level of protection is ensured in the third country, a territory or one or more specified sectors within that third country, or within the international organisation and the personal data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

2. The Union institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 1.

3. The Union institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 45(3) and (5) of Regulation (EU) 2016/679, that a third country or an international organisation ensures or no longer ensures an adequate level of protection.

Article 49
Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:

   (a) a legally binding and enforceable instrument between public authorities or bodies;

   (b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 70(2);

   (c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 70(2);

   (d) binding corporate rules, codes of conduct and certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

   (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

   (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.

5. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.

Article 50
Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 51
Derogations for specific situations

1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679, or of appropriate safeguards pursuant to Article 49, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

   (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

   (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;

   (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;

   (d) the transfer is necessary for important reasons of public interest;

   (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 of other persons, 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 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 a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.

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, unless authorised by Union law. Where 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. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law.

4. In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.

5. The Union institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where this Article has been applied.

Article 52
International cooperation for the protection of personal data

In relation to third countries and international organisations, the European Data Protection Supervisor, in cooperation with the Commission and the European Data Protection Board, shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective 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 cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

THE EUROPEAN DATA PROTECTION SUPERVISOR

Article 53
European Data Protection Supervisor

1. The European Data Protection Supervisor is hereby established.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, is respected by the Union institutions and bodies.

3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends the European Data Protection Supervisor shall fulfil the tasks provided for in Article 58 and exercise the powers granted in Article 59.

Article 54

Appointment of the European Data Protection Supervisor

1. The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public. On the basis of the list drawn up by the Commission, the competent committee of the European Parliament may decide to hold a hearing in order to enable it to express a preference.

2. The list drawn up by the Commission from which the European Data Protection Supervisor shall be chosen shall be made up of persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities established under Article 41 of Regulation (EU) 2016/679.

3. The term of office of the European Data Protection Supervisor shall be renewable once.

4. The duties of the European Data Protection Supervisor shall cease in the following circumstances:

   (a) if the European Data Protection Supervisor is replaced;

   (b) if the European Data Protection Supervisor resigns;

   (c) if the European Data Protection Supervisor is dismissed or required to take compulsory retirement.

5. The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice of the European Union at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.

6. In the event of normal replacement or voluntary resignation, the European Data Protection Supervisor shall nevertheless remain in office until he or she has been replaced.

7. Articles 11 to 14 and 17 of the Protocol on the Privileges and Immunities of the European Union shall apply to the European Data Protection Supervisor.

Article 55

Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources

1. The European Data Protection Supervisor shall be considered equivalent to a judge of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.

2. The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.

3. The budget of the European Data Protection Supervisor shall be shown in a separate budget heading in Section IX of the general budget of the European Union.

4. The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure.

5. The officials and the other staff members of the Secretariat of the European Data Protection Supervisor shall be subject to the rules and regulations applicable to officials and other servants of the European Union.

6. The European Data Protection Supervisor shall have its seat in Brussels.

Article 56
Independence

1. The European Data Protection Supervisor shall act with complete independence in performing his or her tasks and exercising his or her powers in accordance with this Regulation.

2. The European Data Protection Supervisor shall, in the performance of his or her tasks and exercise of his or her powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.

4. The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and benefits.

Article 57
Professional secrecy

The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

Article 58
Tasks

1. Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:

   (a) monitor and enforce the application of this Regulation and other Union acts relating to the protection of natural persons with regard to the processing of personal data by a Union institution or body, with the exception of the processing of personal data by the Court of Justice of the European Union acting in its judicial capacity;

   (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) promote the awareness of controllers and processors of their obligations under this Regulation;

(d) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in Member States to that end;

(e) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(f) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(g) advise all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;

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

(i) adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 49(2);

(j) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);

(k) participate in the activities of the European Data Protection Board set up by Article 68 of Regulation (EU) 2016/679;

(l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;

(m) give advice on the processing referred to in Article 40(2);

(n) authorise contractual clauses and provisions referred to in Article 49(3);

(o) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 59(2);

(p) fulfil any other tasks related to the protection of personal data; and

(q) establish his or her Rules of Procedure.

2. The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 59
Powers

1. The European Data Protection Supervisor shall have the following investigative powers:

   (a) to order the controller and the processor to provide any information it requires for the performance of its tasks;

   (b) to carry out investigations in the form of data protection audits;

   (c) to notify the controller or the processor of an alleged infringement of this Regulation;

   (d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

   (e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law;

2. The European Data Protection Supervisor shall have the following corrective powers:

   (a) to issue warnings to a controller or processor that the intended processing operations are likely to infringe provisions of this Regulation;

   (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

   (c) refer the matter to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;

   (d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

   (e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

   (f) to order the controller to communicate a personal data breach to the data subject;

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

   (h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;

   (i) to impose an administrative fine pursuant to Article 66, subject to non-compliance by the Union institution or body with one of the measures referred to in this paragraph and depending on the circumstances of each individual case;

   (j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.

3. The European Data Protection Supervisor shall have the following authorisation and advisory powers:

   (a) to advise data subjects in the exercise of their rights;

(b) to advise the controller in accordance with the prior consultation procedure referred to in Article 40;

(c) to issue, on its own initiative or on request, opinions to the Union institutions and bodies and to the public on any issue related to the protection of personal data;

(d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 49(2);

(e) to authorise contractual clauses referred to in point (a) of Article 49(3);

(f) to authorise administrative arrangements referred to in point (b) of Article 49(3);

4. The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union law.

5. The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice of the European Union under the conditions provided for in the Treaty and to intervene in actions brought before the Court of Justice of the European Union.

Article 60
Activities report

1. The European Data Protection Supervisor shall submit an annual report on its activities to the European Parliament, the Council and the Commission and at the same time make it public.

2. The European Data Protection Supervisor shall forward the activities report to the other Union institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament.

CHAPTER VII

COOPERATION AND CONSISTENCY

Article 61
Cooperation with national supervisory authorities

The European Data Protection Supervisor shall cooperate with supervisory authorities established under Article 41 of Regulation (EU) 2016/679 and Article 51 of Directive (EU) 2016/680 (hereinafter "national supervisory authorities") and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA[21] to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, requesting national supervisory authorities to exercise their powers or responding to a request from such authorities.

[21] Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323, 10.12.2009, p. 20–30.

Article 62

Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities

1. Where a Union act refers to this Article, the European Data Protection Supervisor shall cooperate actively with the national supervisory authorities, in order to ensure effective supervision of large IT systems or Union agencies.

2. The European Data Protection Supervisor shall, acting within the scope of its respective competences and in the framework of its responsibilities, exchange relevant information, assist in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights, as necessary, jointly with the national supervisory authorities.

3. For the purposes laid down in paragraph 2, the European Data Protection Supervisor shall meet with the national supervisory authorities at least twice a year within the framework of the European Data Protection Board. The costs and servicing of those meetings shall be borne by the European Data Protection Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

4. A joint report of activities as regard coordinated supervision shall be sent by the European Data Protection Board to the European Parliament, the Council, and the Commission every two years.

CHAPTER VIII

REMEDIES, LIABILITY AND PENALTIES

Article 63

Right to lodge a complaint with the European Data Protection Supervisor

1. Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The European Data Protection Supervisor shall inform the data subject of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 64.

3. If the European Data Protection Supervisor does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the complaint shall be deemed to have been rejected.

Article 64

Right to an effective judicial remedy

The Court of Justice of the European Union shall have jurisdiction to hear all disputes relative to the provisions of this Regulation, including claims for damages.

Article 65
Right to compensation

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaties.

Article 66
Administrative fines

1. The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to points (d) to (h) and (j) of Article 59(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

   (b) any action taken by the Union institution or body to mitigate the damage suffered by data subjects;

   (c) the degree of responsibility of the Union institution or body taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;

   (d) any similar previous infringements by the Union institution or body;

   (e) the degree of cooperation with the European Data Protection Supervisor, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

   (f) the categories of personal data affected by the infringement;

   (g) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement;

   (h) where measures referred to in Article 59 have previously been ordered against the Union institution or body concerned with regard to the same subject-matter, compliance with those measures.

The proceedings leading to the imposition of those fines should be carried out in a reasonable timeframe according to the circumstances of the case and taking into account the relevant actions and proceedings referred to in Article 69.

2. Infringements of the obligations of the Union institution or body pursuant to Articles 8, 12 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 and 46 shall, in accordance with paragraph 1, be subject to administrative fines up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year.

3. Infringements of the following provisions by the Union institution or body shall, in accordance with paragraph 1, be subject to administrative fines up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 4, 5, 7 and 10;

(b) the data subjects' rights pursuant to Articles 14 to 24;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 47 to 51.

4. If a Union institution or body, for the same or linked or continuous processing operations, infringes several provisions of this Regulation or the same provision of this Regulation several times, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

5. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution or body which is the subject of the proceedings conducted by the Supervisor the opportunity of being heard on the matters to which the Supervisor has taken objection. The European Data Protection Supervisor shall base its decisions only on objections on which the parties concerned have been able to comment. Complainants shall be associated closely with the proceedings.

6. The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

7. Funds collected by imposition of fines in this Article shall be the income of the general budget of the European Union.

Article 67
Representation of data subjects

The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.

Article 68
Complaints by Union staff

Any person employed by a Union institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of this Regulation, without acting through official channels. No one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging such an infringement.

Article 69
Sanctions

Any failure to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Union liable to disciplinary or any other action, in accordance with the rules and

procedures laid down in the Staff Regulations of Officials of the European Union or in the Conditions of Employment of Other Servants of the European Union.

CHAPTER IX

IMPLEMENTING ACTS

Article 70
Committee procedure

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. 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.

CHAPTER X

FINAL PROVISIONS

Article 71
Repeal of Regulation (EC) No 45/2001 and of Decision No 1247/2002/EC

Regulation (EC) No 45/2001 [22] and Decision No 1247/2002/EC[23] are repealed with effect from 25 May 2018. References to the repealed Regulation and Decision shall be construed as references to this Regulation.

Article 72
Transitional measures

1. The Decision 2014/886/EU of the European Parliament and of the Council[24] and the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation.

2. The Assistant Supervisor shall be considered equivalent to the Registrar of the Court of Justice of the European Union as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.

3. Article 54(4), (5) and (7), and Articles 56 and 57 of this Regulation shall apply to the current Assistant Supervisor until the end of his term of office on 5 December 2019.

4. The Assistant Supervisor shall assist the European Data Protection Supervisor in all the latter's duties and act as a replacement when the European Data Protection Supervisor is absent or prevented from attending to those duties until the end of the Assistant Supervisor's term of office on 5 December 2019.

---

22 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 8, 12.1.2001.

23 Decision No 1247/2002/EC of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties, OJ L 183, 12.07.2002, p. 1

24 Decision 2014/886/EU of the European Parliament and of the Council of 4 December 2014 appointing the European Data Protection Supervisor and the Assistant Supervisor, OJ L 351, 09.12.2014, p.9.

Article 73
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 from 25 May 2018.

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 mode(s) planned

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 contributions

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 of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

1.2. Policy area(s) concerned in the ABM/ABB structure[25]

Justice – Protection of Personal Data

1.3. 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**[26]

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

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

1.4. Objective(s)

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

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 establish a comprehensive data protection framework covering all areas.

On 27 April 2016, the Union has adopted the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

On the same day, the Union has adopted the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

This proposal aims at completing the establishment of a comprehensive data protection framework in the Union, by aligning the data protection rules applicable to Union institutions and bodies with the data protection rules of the Regulation (EU) 2016/679. For reasons of consistency and coherence, Union institutions and bodies

[25] ABM: activity-based management; ABB: activity-based budgeting.

[26] As referred to in Article 54(2)(a) or (b) of the Financial Regulation.

should apply a similar set of data protection rules as the public sector in the Member States.

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

Specific objective No 1:

To ensure consistent application of data protection rules throughout the Union.

Specific objective No 2:

To rationalise the current governance model of data protection in Union institutions and bodies.

Specific objective No 3:

To ensure stronger compliance with and enforcement of data protection rules in Union institutions and bodies.

1.4.3. Expected result(s) and impact

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

As regards Union institutions and bodies as data controllers, they should benefit from the shift from the current (ex ante approach) administrative processes related with data protection towards effective compliance and stronger enforcement of substantive data protection rules and the new data protection principles and concepts introduced by the Regulation (EU) 2016/679 (ex post approach), which will be applicable throughout the Union.

Individuals whose data are being processed by Union institutions and bodies will enjoy better control of their personal data and trust the digital environment. They will also encounter reinforced accountability of Union institutions and bodies.

The European Data Protection Supervisor will be able to focus more on its supervisory role. The distribution of task of giving advice to the Commission between the European Data Protection Board established by Regulation (EU) 2016/679 and the European Data Protection Supervisor will be clarified and duplications will be avoided.

1.4.4. Indicators of results and impact

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

Indicators shall include the following elements:

number of opinions issued by the European Data Protection Board and the European Data Protection Supervisor,

breakdown of activities of data protection officers,

use made of data protection impact assessments,

number of complaints made by data subjects,

fines imposed on data controllers responsible for breaches of data protection.

1.5. Grounds for the proposal/initiative

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

In Regulation (EU) 2016/679 (Article 2(3), Article 98, recital 17) the Union co-legislators called for adapting Regulation (EC) No 45/2001 to the principles and rules established in Regulation (EU) 2016/679 in order to provide a strong and coherent data protection framework in the Union and to allow application of both instruments at the same time, i.e. on 25 May 2018.

1.5.2. Added value of EU involvement

The data protection rules applicable to Union institutions and bodies can be introduced only by way of an EU act.

1.5.3. Lessons learned from similar experiences in the past

The present proposal builds on the experience with Regulation (EC) No 45/2001 and the assessment of its application, carried out in an Evaluation Study (conducted by an external contractor between September 2014 and June 2015).[27]

1.5.4. Compatibility and possible synergy with other appropriate instruments

The present proposal builds on the Regulation (EU) 2016/679 and finalises the building of a strong, consistent and modern data protection framework in the Union – technologically neutral and future proof.

[27] JUST/2013/FRAC/FW/0157/A4 in the context of the multiple framework contract JUST/2011/EVAL/01 (RS 2013/05) - Evaluation Study on Regulation (EC) 45/2001, by Ernst and Young

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

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

– ☐ Financial impact from YYYY to YYYY

- Proposal/initiative of **unlimited duration**
- Implementation with a start-up period from [2017] to 25 May 2018, followed by full-scale operation.

1.7. Management mode(s) planned[28]

- Direct management by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 208 and 209 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

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

Comments

This proposal is limited to and affects all Union institutions and bodies.

[28] 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

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

This proposal is limited to the application of data protection rules by Union institutions and bodies. The supervision and enforcement of those rules is a task carried out by the European Data Protection Supervisor. The monitoring and reporting is therefore provided by the European Data Protection Supervisor. In particular, under Article 60 of this proposal, the European Data Protection Supervisor has the obligation to submit an annual report on activities falling within its competence to the European Parliament, the Council and the Commission and at the same time to make it public.

2.2. Management and control system

2.2.1. Risk(s) identified

An Evaluation Study of the application of the Regulation (EC) No 45/2001 has been carried out by an external contractor, between September 2014 and June 2015. It also looks at the impact of introducing the key concepts and principles of Regulation (EU) 2016/679 in the Union institutions and bodies. The new data protection model will focus on effective compliance with the data protection rules and the effective supervision and enforcement of those rules. It will require a shift of data protection culture in the Union institutions and bodies, moving from the administrative *ex ante* approach to the effective *ex post* approach.

2.2.2. Information concerning the internal control system set up

Existing control methods applied by the Union institutions and bodies.

2.2.3. Estimate of the costs and benefits of the controls and assessment of the expected level of risk of error

Existing control methods applied by the Union institutions and bodies.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

Existing fraud prevention methods applied by the Union institutions and bodies.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Heading……..……]	Diff./Non-diff.[29]	from EFTA countries [30]	from candidate countries[31]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Heading……]	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	[XX.YY.YY.YY]		YES/NO	YES/NO	YES/NO	YES/NO

29 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

30 EFTA: European Free Trade Association.

31 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3.2. Estimated impact on expenditure

The impact on expenditure of this proposal is limited to the expenditure of Union institutions and bodies. However, the evaluation of the costs linked to this proposal shows that it does not create substantial additional expenditure for Union institutions and bodies.

As regards data controllers in Union institutions and bodies, the evaluation study of the Regulation (EC) No 45/2001 shows that their data protection activities correspond to around 70 Full Time Equivalents (FTEs), i.e. around 9.3 million euros per year. Around 20% of their data protection activities are currently devoted to notifications of data processing. This activity is abolished in the present Regulation, corresponding to the annual savings of EUR 1.922 million for data controllers in Union institutions and bodies. These savings is expected to be offset by increased investment of data controllers in the implementation of the new principles and concepts introduced by the present Regulation.

More precisely, the survey carried out in the framework of the evaluation study pointed out that the introduction of:

a) the principle of data minimisation would result in a minimal or non-existent impact on Union institutions and bodies;

b) the principle of transparency would not have a significant impact on Union institutions and bodies;

c) the increased information obligations would increase the workload of data controllers and data protection officers;

d) the right to be forgotten would not have a significant impact on Union institutions and bodies;

e) the right to data portability would result in a minimal or non-existent impact on Union institutions and bodies;

f) data protection impact assessments would have a moderately significant on the workload of data controllers and data protection officers, because some Union institutions and bodies already carry out data protection impact assessments and the instances in which such data protection impact assessments will have to be carried out are limited;

g) notifications of personal data breaches would increase the workload of data controllers, but such breaches are not frequent;

h) data protection by design and data protection by default are already in use in several Union institutions and bodies.

Furthermore, the impact assessment carried out before the adoption of the proposal for a data protection reform package concluded that "no administrative burden would be incurred by either public authorities or data controllers as a result of the introduction of the data protection by design principle."[32]

---

[32] Commission staff working document, Impact Assessment, SEC (2012) 72 final, page 110.

As regards the data protection officers, the evaluation study estimated the cost of the current network of data protection officers and data protection coordinators (DPOs and DPCs) in Union institutions and bodies at 82.9 FTEs or EUR 10.9 million per year. They spend 26% of their data-protection-related time on activities abolished by the present Regulation, i.e. drafting notifications (instead of data controllers), assessing the notifications received and keeping their records in the register and performing prior checks. This leads to further savings of EUR 2.834 million per year for Union institutions and bodies. Moreover, the present Regulation makes room for potential additional savings by allowing Union institutions and bodies to outsource DPO activities, instead of employing their own staff.

The savings in respect of DPO activities will be offset by their involvement in increased information obligations, data protection impact assessments (in limited circumstances when they will be required) and in prior consultation of the European Data Protection Supervisor (the scope of which will be much more limited than the current obligation of prior checking).

As regards the European Data Protection Supervisor, its yearly budget is fairly stable since 2011 and revolves around EUR 8 million. Currently, its Supervision and enforcement unit and its Policy and consultation unit have similar staff numbers, stable since 2008. The increased focus of the present Regulation on the supervisory role of the European Data Protection Supervisor will be offset by more targeted advisory role and the removal of duplication of tasks with the European Data Protection Board. A re-allocation of staff of the European Data Protection Supervisor can be therefore accomplished internally.

This proposal foresees a possibility for the European Data Protection Supervisor to impose administrative fines on Union institutions and bodies. Each Union institution or body can be fined up to a maximum amount of EUR 250 000 per year (EUR 25 000 per infringement), or EUR 500 000 per year (EUR 50 000 per infringement) for the gravest infringements of this Regulation. Such fines are expected to be applied only in most serious cases, and following the non-compliance of the Union institution or body with the exercise of other corrective powers by the European Data Protection Supervisor. It is therefore expected that the financial impact of such fines is limited.

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	[Heading……...…….]

DG: <…….>			Year **N**[33]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration	**TOTAL**

[33] Year N is the year in which implementation of the proposal/initiative starts.

							of the impact (see point 1.6)			
• Operational appropriations										
Number of budget line	Commitments	(1)								
	Payments	(2)								
Number of budget line	Commitments	(1a)								
	Payments	(2a)								
Appropriations of an administrative nature financed from the envelope of specific programmes[34]										
Number of budget line		(3)								
TOTAL appropriations for DG <…….>	Commitments	=1+1a +3								
	Payments	=2+2a +3								

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING <….> of the multiannual financial framework	Commitments	=4+ 6								
	Payments	=5+ 6								

If more than one heading is affected by the proposal / initiative:

[34] 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.

• 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								
	Payments	=5+ 6								

Heading of multiannual financial framework	**5**	'Administrative expenditure'

EUR million (to three 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**
DG: <…….>							
• Human resources							
• Other administrative expenditure							
TOTAL DG <…….>	Appropriations						

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)								

EUR million (to three decimal places)

		Year **N**[35]	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 of the multiannual financial framework	Commitments								
	Payments								

35 Year N is the year in which implementation of the proposal/initiative starts.

3.2.2. Estimated impact on operational appropriations

- The proposal/initiative does not require the use of operational appropriations

☐ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			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**	
			OUTPUTS															
	Type[36]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[37]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTAL COST																		

[36] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[37] As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.3.1. Summary

- The proposal/initiative does not require the use of appropriations of an administrative nature

☐ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **N** [38]	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								
Other administrative expenditure								
Subtotal HEADING 5 of the multiannual financial framework								
Outside HEADING 5 [39] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 5 of the multiannual financial framework								
TOTAL								

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that 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.

---

38 Year N is the year in which implementation of the proposal/initiative starts.

39 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.

3.2.3.2. Estimated requirements of human resources

- The proposal/initiative does not require the use of human resources.

☐ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		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 staff)								
XX 01 01 01 (Headquarters and Commission's Representation Offices)								
XX 01 01 02 (Delegations)								
XX 01 05 01 (Indirect research)								
10 01 05 01 (Direct research)								
• External staff (in Full Time Equivalent unit: FTE)[40]								
XX 01 02 01 (AC, END, INT from the 'global envelope')								
XX 01 02 02 (AC, AL, END, INT and JED in the delegations)								
XX 01 04 **yy** [41]	- at Headquarters							
	- in Delegations							
XX 01 05 02 (AC, END, INT - Indirect research)								
10 01 05 02 (AC, END, INT - Direct research)								
Other budget lines (specify)								
TOTAL								

XX is the policy area or budget title concerned.

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.

Description of tasks to be carried out:

Officials and temporary staff	
External staff	

40 AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JED= Junior Experts in Delegations.

41 Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.4. Compatibility with the current multiannual financial framework

- The proposal/initiative is compatible the current multiannual financial framework.

☐ The 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.

☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

- The proposal/initiative does not provide for co-financing by third parties.

The proposal/initiative provides for the co-financing estimated below:

Appropriations in EUR million (to three 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 co-financed								

3.3. Estimated impact on revenue

- The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on miscellaneous revenue

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[42]						
		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)		
Article …….								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

Specify the method for calculating the impact on revenue.

[42] 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.