COUNCIL OF THE EUROPEAN UNION

Brussels, 22 June 2012

11326/12

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 75
JAI 423
MI 437
DRS 93
DAPIX 70
FREMP 93
COMIX 380
CODEC 1658

NOTE

from:	the Presidency
to:	Working Party on Data Protection and Exchange of Information
No Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Following the DAPIX meetings of 23-34 February and 14-15 March 2012 and in the light of the written comments provided by Member States[1], the Presidency has revised the draft regulation proposed by the Commission. The proposed changes regard Articles 1-10 and 80(a) and 83.
All delegations have a general scrutiny reservation on this proposal and the following delegations have a parliamentary scrutiny reservation: CZ, HU, NL and PL.

Almost all delegations are of the opinion that the proposed regulation contains too many cases of delegated acts. Several delegations have a reservation on the chosen legal form of the proposed instrument and would prefer a Directive[2].

---

1 9897/1/12 REV 1 DATAPROTECT 59 JAI 332 MI 331 DRS 79 DAPIX 63 FREMP 72 COMIX 296 CODEC 1296

2 BE, CZ, DE, SI.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) and Article 114(1) 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[3],

After consulting the European Data Protection Supervisor[4],

Acting in accordance with the ordinary legislative procedure,

Whereas:

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

---

3 OJ C , , p. .

4 OJ C , , p. .

(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.

(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

(3a) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity[6].

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

---

5 OJ L 281, 23.11.1995, p. 31.

6 The Presidency suggests moving former recital 139 up here so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.

(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.

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

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.

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

(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern 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, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.

(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.

(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, (…) or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(14a) This Regulation does not cover the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/20017 and other Union legal instruments covering such processing of personal data should be adapted to the principles and rules of this Regulation, taking into account the specific nature of that processing.

---

7 OJ L 8, 12.1.2001, p. 1.

(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic (…)[8]and without any gainful interest and thus without any connection with a professional or commercial activity. The Regulation should (…) not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.[9]

(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY)[10].

(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Personal data in documents held by a public authority or a public body may be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject, and the data subject's legitimate interests or fundamental rights and freedoms in the particular case are not prejudiced.

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

---

8 Deleted, as this example was out of date.

9 UK suggests adding: "The number of individuals to whom the data are disclosed shall not of itself determine whether the processing of personal data is conducted by a natural person in the course of an personal or household activity."

10 ES had proposed to add a recital on the processing of personal data by authorities that are competent for drawing up electoral rolls.

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

(21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes[11].

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

(23) The principles of protection should apply to any information concerning an [12]identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual, unless this would involve a disproportionate effort in terms of time or technical or financial resources. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. The principles of data protection should not apply to deceased persons[13].

(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. However, identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances[14].

---

11 UK suggests deleting this recital.

12 UK suggests to clarify that the principle of data protection applies only where the person is easily identifiable.

13 Suggested clarification in accordance with a SE suggestion.

14 DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and FR broadly supported this recital. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. COM clarified that the proposed Regulation went less far than the current ECJ case law (Scarlett C-70/10) in that IP addresses should be considered as persona data only they actually lead to the identification of data subjects. DE queried who would in practice be responsible for such meta data.

(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.

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

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

(30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.

(34) Consent should not provide a valid legal ground for the processing of personal data in a specific case, where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed in such a situation of dependence by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law or in a Member State law. Such laws may determine more precisely the conditions for the processing of personal data within the limits of the provisions of this Regulation. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.

(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.

(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific (…) purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.

(41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

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

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

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

(45) If the 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. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.

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

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

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

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

(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.

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

(54) 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 third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

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

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

(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.

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

(59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.

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

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

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

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.

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

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

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

(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.

(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

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

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

(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

(83) 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 may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority.

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

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

(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State 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 this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

(87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.

(88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific (…) purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

(89) 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 a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. . Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.

(91) When personal data moves across borders it may put at increased risk the ability of individuals 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 may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.

(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.

(94) Each supervisory authority should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.

(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

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

(98) The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.

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

(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.

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

(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.

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

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

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

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

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

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

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

(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

(111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.

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

(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.

(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.

(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.

(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.

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

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

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

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

(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in 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, meaning 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 personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.

(124a) As regards statistics, 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 Communities15 provides further specifications on statistical confidentiality for European statistics.

(125) The processing of personal data for the purposes of historical, statistical or scientific (…) purposes should, in order to be lawful, also respect other relevant legislation such as on clinical trials.

(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.

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

(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.

---

15 OJ L 87, 31.3.2009, p. 164–173.

(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific (…) purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[16]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.

---

[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.

(132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.

(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.

(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.

(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[17].

(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[18].

---

17 OJ L 176, 10.7.1999, p. 36.

18 OJ L 53, 27.2.2008, p. 52.

(138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[19].

(139) (…)[20].

[19] OJ L 160 of 18.6.2011, p. 19.

[20] The Presidency has moved former recital 139 up to recital 3a so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.

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 individuals[21] with regard to the processing of personal data and rules relating to the free movement of personal data[22].

2. This Regulation protects (…) fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data[23].

---

21 AT, supported by LI, thought that a recital should acknowledge Member States' right to lay down the right to data protection rules for legal persons.

22 IT thought that a reference to the internal market should be added here; COM indicated this reference was already included in recital 2. DE, on the other hand, thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to single market implications of the data processing operations.

23 Deletion of "the" in order to allay IE concerns that this paragraph conveyed the impression that the right to data protection enjoyed a higher status than other fundamental rights.

3. (…)[24] [25].

Article 2
Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system[26] [27].

---

[24] Deletion as the Presidency agreed with FR that this paragraph, which was copied from the 1995 Data Protection Directive, did not make sense in the context of a Regulation as this was directly applicable. NL remarked that the drafting did not specify the addressees of this rule. DE scrutiny reservation: queried whether Member States would still be allowed to keep more stringent, sectoral data protection rules in place. The Commission stated that Member States were still allowed to determine more precisely the conditions for the processing of personal data in leges speciales under which provide the legal basis referred to in Article 6(1)(e) and (3), which could however not be more stringent than EU data protection rules. SK thought that this paragraph needed to be redrafted so as to allow processing of personal data from one Member State in another Member State, also in cases where the processing in another Member State was not necessary or reasonable.

[25] EE, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. DE concurred that this was a very important issue which needed to be addressed. The Commission stated that its proposal did not contain rules on the access to public documents as regards the fundamental right aspect, since the Charter only refers thereto regarding the EU institutions.

[26] FR queried the exact meaning of the second half of this sentence. HU objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording "irrespective of the means by which personal data are processed".

[27] BE scrutiny reservation related to the fact that the processing of personal data by judicial authorities would be covered by the Directive.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law[28], and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters);

(b) by the Union institutions, bodies, offices and agencies[29];

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union[30];

(d) by a natural person [without any gainful interest][31] in the course of its own exclusively personal or household activity;

---

28 DE thought the activities covered by Union law should be listed as fully as possible. SE also thought that the utmost clarity was required in this respect.

29 FR wants clarification as to whether transfers of data by Member States to these EU institutions are covered by this exception. The Presidency submits that this exception covers only processing by the institutions and not any data transfers from Member States to the institutions. BE, DE, EE and ES thought the Regulation should be applicable to EU institutions. The Presidency finds that further justification for this exclusion should be provided by COM, at which time the subject should be revisited.

30 IT thought this exception overlapped with (a). COM would reflect on this.

31 DE, IE, NL and UK questioned the need for the criterion of absence of gainful interest in this so-called household exception and the compatibility thereof with the *Lindqvist* case law of the ECJ (which, at any rate, predated the 'social network era'). UK thought that selling personal possessions on an auction site also fall within the household exemption. The enforceability of data protection rules in this type of situation was also challenged. SE thought the household exeception needed to be drafted in a suficiently wide manner so as to ensure the practical enforceability of data protection rules. COM affirmed the compatibility with the *Lindqvist* case law. Several delegations (DE, SE and UK) asked whether the use of social networks on the internet would be covered by this exception. COM replied that in its view the Regulation should apply to an individual who uses a social network and has "with the public" privacy settings, i.e. when personal data are available ith to an unrestricted number of individuals and not only to a limited audience at large. CZ thought that the processing of personal data by a natural person which is not part of its ownn gainful activity should be subjected to limited, specific rules to be spelled out in the Regulation. LU, NO and SK also thought this exception needed to be more clearly regulated. BE would like to add the following recital: “That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.”

(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[32] [33]

3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive[34].

Article 3
Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union[35].

---

32 RO scrutiny reservation: it thought that this exception should be worded more broadly and suggested adding "and ensuring public order and security". FR thought that this exception should be worded more broadly so that it would cover all forms of exercise of 'sovereign power' with a sanctioning goal. FR also thought that the "competent authorities" should be clearly defined. COM replied that point e) should mark the delimitation between the two data protection instruments. DE referred to the difficulties flowing from the fact that the prevention of dangerous situations (*Gefahrenabwehr*) is not covered by the proposed Data Protection Directive, whereas the processing of data in that context is intrinsically linked to other police activities covered by that Directive. At the request of HU, COM clarified that Member States in their national data protection legislation could cover in a single law also data processing in this area.

33 ES proposed to insert two further exemptions for processing by competent authorities for the purposes of producing and disseminating official statistics and of drawing up electoral rolls.

34 FR scrutiny reservation: FR demands clarification as to whether "Business to Business (B2B)" transactions are covered by the proposed Regulation. FR and IT underlined the importance of close alignment of this Regulation with the E-Commerce Directive; IT thought that it was not expedient that the exceptions listed here were broader than under the E-Commerce Directive. DE queries whether also the implementing law of the Member States should be taken into account or also other EU Directives, such as the so-called Cookies-Directive 2002/58/EC.

35 FR accepted this criterion. DE and LV expressed some doubt as to its practicability with regard to corporations in the EU that are active on a worldwide basis. Some delegations thought the criterion of establishment should be better defined (PT), e.g. whether it also applied to natural persons (LV).

2. [36]This Regulation applies to the processing of personal data of data subjects residing in the Union[37] by a controller not established in the Union[38], where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required[39], to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union[40] [41].

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law[42].

---

36 COM stated that this territorial scope stemmed from a human rights obligation to protect EU data subjects also regarding their personal data processed outside the European Union, whose data are processed by a controller not established in the EU..

37 UK remarked that this criterion/condition implied a different data protection regime for the EU establishments of non-EU companies according to whether their customers are EU residents or not. COM indicated it would reflect on this. NO thought the Regulation should also cover the processing done outside the Union by processors established within the Union. At the request of FR, COM clarified that this criterion was intended to apply solely to persons with a residence in the EU, not to persons travelling in the EU.

38 DE, supported by BE, queried whether this would also apply to foreign public authorities (e.g. US DHS) and to endowments or other non-profit associations. COM replied that the Charter made no distinction according that 'nature' of the controller and that possible practical enforcement problems should not deter the EU from laying down clear rules on the rights.

39 Suggested text to allay concerns expressed by DE and PT, that it needed to be clarified that this also covered services offered free of charge.

40 BE, IE, SE and SK scrutiny reservation. Several delegations remarked that this would also apply to some foreign public authorities, e.g. the under the US ESTA programme. IE, SK and SE remarked more clarity was required as to the exact scope of this, pointing out that 'monitoring' encompassed much more than tracking on the internet. COM replied that Recital 21 offered some clarifications in this regard.

41 FR and CZ thought the two subparagraphs should be deleted. FR supported the proposed first sentence of the current paragraph 2, whereas CZ thought one should revert to Article 4(1)(c) of the 1995 Directive. UK would like to see Article 3(2) removed in its entirety. The presidency suggests this rewording. A recital should clarify the precise boundaries of the "monitoring" scope.

42 BE and UK scrutiny reservation: unclear in which cases this article will apply. Cf. Recital 22.

Article 4
Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by means reasonably likely to be used[43] by the controller or by any other natural or legal person, in particular by reference to a name[44], an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[45]. If identification requires a disproportionate amount of time, effort or material resources the natural living person shall not be considered identifiable.[46];

(2) (…) [47];

---

43 FR, LU and UK thought that this concept was too broad.

44 SE proposal.

45 IE and LU scrutiny reservation: this extended scope lacks legal certainty and takes no account of the intended purpose, context, circumstances or likely privacy impact of processing the personal data concerned. It has not been sufficiently demonstrated that the existing definition of 'personal data' in article 2(a) of Directive 95/46 needs to be replaced. UK thought it was preferable to list these examples in an exemplary manner in a recital rather than in the operative body of the text. FR and UK thought the definition of personal data rather than of data subject should be determining

46 The Presidency suggests this addition, however further reflection may be needed in order to establish to whom the identification must be disproportionate. To the original data controller, identification will most likely never be disproportionate, but this may be the case for third parties that e.g. only see an id number or some other "abstract identifier", which they cannot use to identify the data subject.

47 DE, EE, FI, FR and IT thought that the definition of personal data was no longer compatible with the digitalised age in which even satellite images could fall under this definition. AT however thought that so-called geo data could be the subject of specific sectoral rules. FR and HU proposed to clarify, as is the case under the 1995 Directive, that the data concern an identified or identifiable data subject. DE, IE, ES, LU, SE and SK queried why anonymisation and/or pseudonymisation techniques were not covered and defined here: anonymised data should not be covered by the Regulation. COM referred to Recital 23 which excluded truly anonymised data from the scope of the Regulation. CZ proposed to insert the following definition: (2a) 'pseudonymous data' means any data where determination of the identity of the data subject requires a disproportionate amount of time, effort, or material resources. SK also thinks greater clarity is required, also in distinguishing the terms 'personal data' and 'information'.

(3) 'processing' means any[48] operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage[49], adaptation or alteration, retrieval, consultation, use, disclosure[50] by transmission, dissemination or otherwise making available, alignment or combination, erasure[51] or destruction[52];

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis[53];

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions[54] and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law[55];

---

48 BE and FR scrutiny reservation: FR thought that this concept was too broad in view of the wide variety of data processing operations possibly covered by this. Read in conjunction with Article 28, this definition would increase rather than reduce administrative burdens on companies. BE thought that the rules applicable to s et of operation should more stringent than those for "any operation".

49 CY queried what was the difference between 'storage' and 'retention' of data.

50 SK thought the list should also include 'making public' and 'copying'. The Presidency submits these two concepts are already covered by the proposed definition. DE also thought further defining might be necessary.

51 DE and NL regretted that the blocking of data was not included in the list of data processing operations as this was a means especially useful in the public sector. COM indicated that the right to have the processing restricted in certain cases was provided for in Article 17(4) (the right to be forgotten), even though the terminology “blocking” was not used there. DE thought the definition of Article 4(3) (erasure) should be linked to Article 17.

52 DE was of the opinion that a separate definition of 'publication of personal data' was required.

53 DE, FR SI, SK and UK scrutiny reservation. DE and SI thought this was completely outdated concept. COM explained that the definition had been taken over from Directive 95/46/EC and is related to the technical neutrality of the Regulation, as expressed in Article 2(1). .. DE also thought a recital should clarify the cases covered by this, e.g. in the context of social networks.

54 UK suggests deleting the reference to the conditions, as this is normally for the processor to determine, not for the controller. UK suggests reverting to the formulation under the 1995 Directive.

55 DE scrutiny reservation on paragraphs 3 to 5: the practical applicability of these definitions in the context of new health services such as Google-health.

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[56];

(7) 'recipient' means a natural or legal person, public authority, agency or any other body[57] to which the personal data are disclosed whether a third party or not[58];

(8) 'the data subject's consent' means any freely given specific, informed and explicit[59] indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action[60], signifies agreement to personal data relating to them being processed[61];

---

56 CZ reservation: CZ wants to delete this definition as it considers the distinction between controller and processor as artificial.

57 HU proposal to add: 'other than the data subject, the data controller or the data processor'.

58 DE, FR and SE regretted the deletion from the 1995 Data Protection Directive of the reference to third party disclosure and pleaded in favour of its reinstatement. COM argued that this reference was superfluous and that its deletion did not make a substantial difference UK scrutiny reservation on the deletion - from the 1995 Directive - of the phrase: 'authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients'.

59 AT, BE, CZ, CY, IE, FR, FI, LT, LU SE, SI, SK and UK scrutiny reservation. Many of these delegations criticised the additional requirements to consent as unrealistic and queried its added value. LU wondered whether an over-regulation of consent by the EU legislator would not deprive the courts of possibilities to intervene in cases where consent would meet all the legal requirements, but might in reality still be inadequate. In the same vein, IE wondered whether the proposed requirements would in reality not lead to 'click fatigue'. DE stated that the conditions for electronic consent should be set out here. CZ proposed to replace the word 'explicit' by 'provable'.COM argued that this definition merely clarified the 1995 Directive concept of consent, which does not allow for silent or implicit consent. IE disagreed that the subjective requirement of informed consent was already present under the 1995 Directive. COM referred to recital 25 for clarifying that consent should not be unnecessarily disruptive to the use of the service for which it is provided.

60 HU suggests adding 'made in writing or by any other recorded means'.

61 DE rejected a 'one-size-fits-all' solution.

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful (…) loss, alteration, unauthorised disclosure of, or [62]access to, personal data transmitted, stored or otherwise processed[63];

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual which have been inherited or acquired during early prenatal development as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained[64 65;]

(11) ['biometric data' means any personal data resulting from a specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which contributes to (…) unique identification of that individual[66], such as facial images, or dactyloscopic data[67];][68]

---

62 ES proposed adding the word 'illegal'; the Presidency however thinks this is covered by the term 'unauthorised'.

63 COM explained that it sought to have a similar rule as in the E-Privacy Directive. LU supports this goal. DE questioned the very broad scope of the duty of notifying data breaches, which so far under German law was limited to sensitive cases. NL, LV and PT concurred with DE and thought this could lead to over-notification. On the other hand HU and SK preferred a broader definition that covers each and every incidents stemming from the breach of the provisions of the regulation. HU therefore suggests amending the definition as follows '…a breach of security the provisions of this regulation leading to any unlawful operation or set of operations performed upon personal data such as ….'. CZ also proposed to refer to a 'security breach' rather than a 'personal data breach'.

64 Several delegations (BE, CH, CY, DE, FR and SE) expressed their surprise regarding the breadth of this definition, which would also cover data about a person's physical appearance. DE thought the definition should differentiate between various types of genetic data. AT scrutiny reservation.

65 The Presidency suggests narrowing the definition to accommodate the concerns expressed by several Member States. The redraft seeks to make definition dependent on a biological – and therefore presumably technologically neutral concept (DNA) – indicator.

66 FR scrutiny reservation. CZ proposal to replace this wording by "…and individual which are unique for each individual specifically…"

67 SI did not understand why genetic data were not included in the definition of biometric data. AT scrutiny reservation. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. DE thought that the signature of the data subject should be exempted from the definition.

68 The Presidency has considered the wording of this provision and proposes the stated text. However, it is the considered view of the Presidency that further reflection is needed in regard to the wording of this provision.

(12) ['data concerning health' means such information related to the physical or mental health of an individual, which reveal significant information about health problems, treatments and sensitive conditions of an[69] individual[70]];

(13) 'main establishment' means

- as regards the controller the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union

- as regards the processor the place of its central administration in the European Union, and if it has no central administration in the European Union the main establishment is the place where the main processing activities take place;

- as regard any natural or legal person, public authority, agency or any other body which acts both as a controller and as a processor, 'main establishment' means the place where it is determined to have its main establishment in its capacity of controller; [71] [72]

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority, [data subject] and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation[73];

---

69 CZ proposal

70 CZ, DE, EE and FR expressed their surprise regarding the breadth of this definition. AT and BE scrutiny reservation. Presidency proposal to allay the concerns raised.

71 BE, CZ DE, EE, IE and SK scrutiny reservation: they expressed concerns about this definition, which might be difficult to apply in practice. DE thought it needed to be examined in conjunction with the one-stop-shop rules in Article 51. IE remarked this place may have no link with the place where the data are processed. IE therefore would prefer to refer to the location of the processor's primary data processing centre; if this location lies outside the Union, the reference should be to the location in the Union where the main decisions are taken (as in the case of controllers). DE also remarked that in the latter scenario, the Commission proposal did not determine which Member States' DPA would be competent. CZ thought the definition should be deleted.

72 The Presidency suggests these amendments to clarify how this concept is applied.

73 SK scrutiny reservation: unclear whether this definition is linked to Article 25.

(15) 'enterprise' means any entity engaged in an[74] economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly[75] engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings[76];

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

(18) (…)[77];

(19) 'supervisory authority' means a[78] public authority which is established by a Member State in accordance with Article 46;

(20) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(21) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[79] [80] [81].

---

74 DE proposed to add the requirement "independent".

75 SE criticised the term 'regularly'. It was also queried why the term 'enterprise' was used here, whereas subparagraph 16 used the term 'undertaking' (as in competition law).

76 UK scrutiny reservation.

77 As the Presidency saw no need for this definition next to Article 8 (cf. NL and UK scrutiny reservation). The Presidency suggests that the need for further precision or definition will be examined in the context of the relevant articles. CZ had proposed adding the words 'under-age/minor'.

78 FR proposal to add 'independent'.

79 OJ L 204, 21.7.1998, p. 37–48.

80 UK suggests adding a definition of "competent authority"corresponding to that of the future Data Protection Directive.

81 BE suggests adding a definition of 'transfer' ('communication or availability of the data to one or several recipients').

CHAPTER II
PRINCIPLES

Article 5
Principles relating to personal data processing

Personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject[82];

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[83]; further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83[84];

(c) adequate, relevant, and limited to the minimum necessary[85] in relation to the purposes for which they are processed; [they shall only be processed if, (…)[86] the purposes could not be fulfilled by processing information that does not involve personal data[87];][88]

---

82 At the request of CY and SI, COM clarified that the transparency principle concerns data processing in relation to data subjects and is further detailed in particular by the information requirements (Articles 11 and 14).. At the request of DE and SE, COM stated that Member States would still be able to adopt/maintain data protection rules under national law within the limits of the Regulation.

83 NL and FI pointed out that too strict rules on processing for other purposes could lead to new data collections for already collected data.

84 Based on BE and UK suggestion.

85 UK suggests to replace 'limited to the minimum necessary" by the terms 'not excessive' (from the 1995 Directive).

86 BE suggestion to delete the words 'as long as', since these create legal uncertainty. BE thought that this test was otherwise impracticable.

87 IE reservation: IE thought the second part of the sentence should be dropped. DE thought that pseudonymised and anonymous data should be mentioned here.

88 The second sentence is deleted as proposed by IE.

(d) accurate and, where necessary[89], kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay[90];

(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 data will be processed (…)[91] for historical, statistical or scientific (…)[92] purposes[93] in accordance with the (…)[94] conditions of Article 83 and if a periodic review[95] is carried out to assess the necessity to continue the storage;

(f) [processed under the responsibility and liability of the controller[96], who shall ensure and be able to[97]demonstrate that the processing of personal data is performed in compliance with the provisions of this Regulation][98].

---

89 CZ, DE, IE, SE and UK thought that the words 'where necessary' from the 1995 Directive should be reinstated. COM replied that it had been deleted because of divergent Member State practice, but that the updating duty was only required in reasonable cases.

90 CZ suggestion to add 'personal data established as inaccurate shall not be disclosed unless rectified or marked appropriately'.

91 UK suggestion to delete the word 'solely' so as to allow for data processing for mixed purposes.

92 Suggestion to delete the word 'research' so as to clarify that also storing of data for historical, statistical or scientific purposes which do not amount to research is possible. This concern was raised by SE and NO.

93 Several delegations (DE, NO, SE and SI) requested clarification as to what would be allowed under this purpose. COM referred to recitals 64 and 126.

94 ES suggestion.

95 LV, NO and UK scrutiny reservation.

96 DE, UK and SI queried the case of joint responsibility between controller and processor.

97 Based on IE, SE and BE suggestion.

98 BE, LU and FR thought turning the existing means obligation into a result obligation was too onerous and not realistic. COM thought the controller should have the burden of proof. DE scrutiny reservation: the exact consequences of this definition are unclear at this stage. ES and UK suggested deleting this element as responsibility and liability is not a condition for data processing, but a consequence thereof. In addition to these concerns the Presidency feels it could be considered firstly, whether all requirements stated in the provision belongs in this Chapter or should rather be moved to Chapter IV and secondly, whether some of the obligations overlap with Article 22 (1).

Article 6

Lawfulness of processing[99]

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

   (a) the data subject has given consent to the processing of their personal data for one or more specific purposes[100];

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

   (c) processing is necessary for compliance with a legal obligation to which the controller is subject[101];

   (d) processing is necessary in order to protect the vital[102] interests[103] of the data subject;

   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[104];

---

99 AT and SK scrutiny reservation...

100 DE and SK asked for an explanation as to the addition of 'for one or more specific purposes'. COM referred to Article 8(2) of the Charter.

101 CH and ES queried the relationship to (e) and HU thought that this subparagraph could be merged with 6(1)(e). BE, CZ and LV were of the opinion that other grounds might be used for data processing in the public sector.

102 IE queried why 'vital' interests were required here, whereas for the public sector only 'legitimate' interests where required.

103 IE suggests to clarify that this includes loss or damage to property. Should perhaps be stated in a recital.

104 COM clarified that this was the main basis for data processing in the public sector. DE asked what was meant by 'public interest' whether the application of this subparagraph was limited to the public sector or could also be relied upon by the private sector.

(f) processing is necessary for the purposes of the legitimate interests[105] pursued by a controller or by a third party[106], except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[107] (…)[108].

(g) purposes and under the conditions provided for in Article 9(2) (b) - (j); [109]

(h) processing is necessary for the purposes and under the conditions referred to in Articles 80 to 85.

2. (…)

---

105 FR scrutiny reservation.

106 In accordance with remarks made by CZ, DE, NL, SE and UK, the Presidency suggests to reinstate the words 'or by a third party' from the 1995 Directive. HU could accept it. COM thought that the use of the concept '***a*** controller' should allow covering most cases of a third party.

107 DE asked whether this would allow an absolute prohibition of processing of children's personal data.

108 As suggested by BE and PT, the Presidency has deleted the last sentence. The Presidency does not believe it can be assumed that all processing carried out by public authorities has a clear legal provision as its basis. The suggested provision would therefore, create real legal uncertainty without any demonstrated added value for citizens. COM was opposed to this as, in its view, the interest on which public authorities act should be determined only by legal provisions.

109 The Presidency has taken the Commissions position as expressed in the Working Party to mean that the processing of data covered by Article 6 can also take place when the conditions in Article 9 are fulfilled. The Presidency suggest inserting this provision as a consequence hereof and to create legal certainty on this issue. The Presidency also finds it most logical and in keeping with the general structure of data protection principles to enable processing of non-sensitive data on "sensitive" grounds. The processing ground in Article 9, 1 (a) is excluded because consent is already stated in Article 6.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law[110], or

(b) the law of the Member State to which the controller is subject.

(…)

4. Where the purpose of further processing is incompatible[111] with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a)[112] to (e) of paragraph 1[113]. This shall in particular apply to any change of terms and general conditions of a contract[114].

5. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child][115].

---

110 ES wondered whether a reference to Union law was needed here as the public interest would (almost) invariably be defined by Member State law.

111 Inserted to make the text compatible with Article 5(b).

112 AT thought that there should be no reference to (1)(b) as the contract itself would be the ground for data processing if its terms allowed for a change of purpose of data processing.

113 ES and LU though it need further clarification which were non-compatible purposes. COM replied that it wanted to improve the situation under the 1995 Directive, which leads to legal uncertainty. DE and PT reservation: they disagreed with this COM explanation. DE, supported by SE, thought that an exception was needed for publicly available data, e.g. in the context of social networks. To that end it would be preferable if a reference to paragraph 1(f) were also to be included here. PRES indicted that this should be clarified in the text.

114 BE and PL scrutiny reservation. DE thought this last sentence should be rather in a recital. BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to recital 40. BE suggested adding the words 'if the process concerns the data mentioned in Articles 8 and 9'. HU thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here: 'Where personal data relating to the data subject are processed under this provision the controller shall inform the data subject according to Article 14 before the time of or within a reasonable period after the commencement of the first operation or set of operations performed upon the personal data for the purpose of further processing not compatible with the one for which the personal data have been collected.'

115 Reservation by BE, DE, EE, ES, FI, FR, IE, LU, NO, NL, PT, PL, SE and UK. NL thought this empowering was superfluous as there was no need for additional legislation. DE and PL thought that such important rules could not be adopted through a mechanism of delegated acts and wondered what would be the situation in the absence of any delegated acts.

Article 7
Conditions for consent

1. [The (…) burden of proof is on the controller to establish that consent[116] was provided for the purposes[117] of Article 6(1)(a).][118]

2. If the data subject's consent is to be given in the context of a written[119] declaration which also concerns another matter, the requirement to give consent must be presented in a manner which is clearly[120] distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal nor shall it affect the lawfulness of processing of data based on other grounds[121] [122].

---

116 IE remarked that it should be clarified that this was consent as referred to in Article 6(1)(a) and not consent in the context of a contract (Article 6(1)(b)). COM confirmed that this article did not apply to processing on the basis of Article 6(1)(b), to which DE remarked that the data subject might be less protected under contractual law.

117 LU, NL and UK thought this proposed rules put a heavy regulatory burden on companies. DE remarked that one would always need to retain some data for logging purposes. SE requested a clarification (e.g. through a recital) that this did not apply in criminal proceedings.

118 Some delegations question if this is compatible with ECHR.

119 DE suggested adding 'electronic'. The Presidency thought that this addition was not required as it was already covered by the word 'written'.

120 As suggested by ES.

121 The presidency suggests this amendment to clarify that the controller will always have the option of basing a continued processing of data on an alternative processing ground if the relevant provisions are fulfilled. This situation could thus arise where processing can be continued pursuant to e.g. Article 6,(1), (c). See also Article 17,(1),(b), *a contrario*.

122 BE suggests to insert a provision reading: "The controller has to fulfil the data subject's request within a reasonable time period". CZ, LU and SE also thought further clarification was required.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller and this imbalance makes it unlikely that consent was given freely.[123] [124]

[123] The Presidency suggests tightening the drafting and turning the provision in to a more operational "burden of proof" rule. This should ensure that the objective of the provision can still be served without making a very large number of otherwise legitimate consent scenarios illegal.

[124] BE, CZ, DE, EE HU, IE, SE, SI and PL scrutiny reservation. SI referred to the case of asylum seekers whose data were processed in SI on the basis of their consent. COM indicated that this would be excluded by the Data Protection Regulation as such processing does not rely on a freely given consent and should be based on a statutory basis. BE asked whether paragraph 4 could not be limited to the processing of sensitive data. DE, IE and NL pleaded to reconsider this rule, which it considered to be very broad. DE remarked that the absence of dependence should be considered as part of the requirement of freely given consent. HU agreed with the principle but thought its application might be problematic in some cases. FR warned against too much specificity in the recitals and suggested adding: 'and must be replaced by another legal basis such as those provided for in Article 6(1)(a) and (b)'. ES and SK thought consent was never required in the public sector. ES remarked that recital 34 was wrongly drafted. UK suggested deleting paragraph 4 and replacing it by the following recital 'the existence of imbalanced situations should be taken into account in determining whether consent is "freely given, and informed'.

Article 8

Processing of personal data of a child[125]

1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child[126], the processing of personal data of a child below the age of 13 years[127] shall only be lawful if and to the extent that consent as referred to in Article 7[128] is given or authorised by the child's parent or custodian[129]. The controller shall make reasonable efforts to obtain (…)[130] consent, taking into consideration available technology[131].

2. 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[132].

3. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1(…)[133].

---

125 AT and SE scrutiny reservation. CZ and UK reservation: CZ and UK would prefer to see this Article deleted.

126 Several delegations (HU, SE, PT) asked why the scope of this provision was restricted to the the offering of information society services or wanted clarification (DE) whether it was restricted to marketing geared towards children. The Commission clarified that this provision was also intended to cover the use of social networks, insofar as this was not governed by contract law. BE, DE and IE thought that this should be clarified (BE suggested through a recital). HU thought the phrase ' in relation to the offering of information society services directly to a child' should be deleted.

127 Several delegations queried the expediency of setting the age of consent at 13 years: FR, HU, NL, LU, LV and SI. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA).

128 The Presidency, supported by SE, thought that it should be clarified that this applies only if consent is the ground for data processing. DE, supported by NO, opined it could have been integrated into Article 7.

129 IT asked how minors could be represented. FR queried whether this implied that for all other rights minors needed to be represented by their parents/legal guardian.

130 DE suggestion: the burden of proof is regulated in Article 7.

131 PL, PT, SE and UK queried the verifiability of compliance with this obligation.

132 DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law.

133 The Presidency has deleted the last part of the provision as several delegations queried the expediency of (using delegated acts for) setting derogations for SMEs to an obligation aimed at protecting children: CZ, DE, EE, ES, FR, LV, PT and SE. DE thought this should be done through Member State law.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)][134].

Article 9

***Processing of special categories of personal data*[135]**

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or philosphical beliefs[136], trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences[137] or related security measures shall be prohibited.[138]

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

   (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject[139]; or

---

134 LU thinks this paragraph is superfluous.

135 AT, PT and LI scrutiny reservation. DE, supported by CZ and UK, criticised on the concept of special categories of data, which does not cover all sensitive data processing operations. CZ pleaded in favour of a concept of risky processing. SK also thought the criterion should be context based and the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. COM referred to the general discussion on an open versus closed list of sensitive data.

136 CY, FR and AT deplored the deletion of the adjective "philosophical" before "beliefs", as this made the concept too broad. IE also thought this was too vague. COM referred to the wording used in the Charter.

137 As suggested by FR. EE reservation: this should be left to the Member States. NL and AT reservation: the inclusion of suspicion of criminal offences should be considered. At the request of CY, COM clarified that disciplinary convictions were not covered by the list.FR thought the wording of the 1995 Directive should be copied.

138 UK questioned the need for special categories of data. NL thought the list of data was open to discussion, as some sensitive data like those related to the suspicion of a criminal offence, were not included. SE thought the list was at the same time too broad and too strict. SI thought the list of the 1995 Data Protection Directive should be kept. FR and AT stated that the list of special categories should in the Regulation and the Directive should be identical.

139 DE questioned whether one needed consent as a specific basis here, referring also to the complicated interaction between Member State and EU law. FR scrutiny reservation. LU thinks that special categories of data and 'normal' data should not be put on the same footing.

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; 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; or

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects[140]; or

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

(f) processing is necessary for the establishment, exercise or defence of legal claims <u>in court proceedings or otherwise</u>[141]; or

(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81[142]; or

(i) processing is necessary for historical, statistical or scientific (…)[143] purposes[144] subject to the conditions and safeguards referred to in Article 83; or

---

140 HU thinks this subparagraph can be deleted as it overlaps with (a).

141 ES suggests adding <u>'of any kind'</u>.

142 DE and EE scrutiny reservation. BE queried what happened in the case of processing of health data by insurance companies.

143 Suggestion to delete the word 'research' so as to clarify that also storing of data for historical, statistical or scientific purposes which do not amount to research is possible. This concern was raised by SE and NO.

144 ES suggests adding: '<u>or for preliminary official or administrative investigation to determine biological parentage'.</u>

(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority[145].

3. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2][146].

Article 10
Processing not allowing identification

[If the purposes for which a controller processes data do not require the identification of a data subject, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with (…) this Regulation.][147]

145 UK scrutiny reservation as interaction with Article 2(2)(e) is unclear. UK suggests adding 'criminal offences' (cf. 1995 Directive)

146 BE, CZ, DE, ES, LU, SE and UK reservation.

147 DE, FR and UK scrutiny reservation. UK thought this should be clarified in recitals.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY AND MODALITIES

Article 11

Transparent information and communication

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

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

Article 12

Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

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

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

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

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13
Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14
Information to the data subject

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

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

   (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

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

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

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

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

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

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

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

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

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

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

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

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

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

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

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

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

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

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

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 15
Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

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

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

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

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

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

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

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

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

SECTION 3
RECTIFICATION AND ERASURE

Article 16
Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Article 17

Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

   (a) the 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 (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

   (c) the data subject objects to the processing of personal data pursuant to Article 19;

   (d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

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

   (a) for exercising the right of freedom of expression in accordance with Article 80;

   (b) for reasons of public interest in the area of public health in accordance with Article 81;

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

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

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

4. Instead of erasure, the controller shall restrict processing of personal data where:

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

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;

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

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

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

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

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

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

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

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

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

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Article 18
Right to data portability

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

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

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

SECTION 4
RIGHT TO OBJECT AND PROFILING

Article 19
Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

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

Article 20
Measures based on profiling

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

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

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

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

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

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

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

SECTION 5
RESTRICTIONS

Article 21
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) public security;

(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) other public interests 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 and the protection of market stability and integrity;

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

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

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

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22
Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

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

(f) keeping the documentation pursuant to Article 28;

(g) implementing the data security requirements laid down in Article 30;

(h) performing a data protection impact assessment pursuant to Article 33;

(i) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(j) designating a data protection officer pursuant to Article 35(1).

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

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Article 23

Data protection by design and by default

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

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

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

Article 24
Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Article 25
Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

   (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

   (b) an enterprise employing fewer than 250 persons; or

   (c) a public authority or body; or

   (d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

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

Article 26
Processor

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

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

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

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

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

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

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

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

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

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

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

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

Article 27

Processing under the authority of the controller and processor

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

Article 28

Documentation

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

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

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

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

   (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

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

   (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

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

   (h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29
Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

SECTION 2
DATA SECURITY

Article 30
Security of processing

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

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

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

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

   (a) prevent any unauthorised access to personal data;

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

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

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

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

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

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

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

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

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

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

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

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

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

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

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

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

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

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33
Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations in particular present specific risks referred to in paragraph 1:

   (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

   (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

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

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

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

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

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

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

Article 34

Prior authorisation and prior consultation

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

   (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

   (b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

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

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

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

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

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

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

SECTION 4
DATA PROTECTION OFFICER

Article 35
Designation of the data protection officer

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

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

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

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

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

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

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

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

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

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

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

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

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

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

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37

Tasks of the data protection officer

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

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

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

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

   (d) to ensure that the documentation referred to in Article 28 is maintained;

   (e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

   (f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

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

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

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

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38
Codes of conduct

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

   (a) fair and transparent data processing;

   (b) the collection of data;

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

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

   (e) information and protection of children;

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

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

   (h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

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

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

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

Article 39
Certification

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

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

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

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

Article 40
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 may only take place 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.

Article 41

Transfers with an adequacy decision

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

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

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

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

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

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

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

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

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

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

   (a) binding corporate rules in accordance with Article 43; or

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

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or

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

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

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Article 43

Transfers by way of binding corporate rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

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

(b) expressly confer enforceable rights on data subjects;

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

2. The binding corporate rules shall at least specify:

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

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

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

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

(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

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

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

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

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

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

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

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

Article 44
Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

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

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

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

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

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

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

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

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

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

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

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

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Article 45

International co-operation for the protection of personal data

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

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

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

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

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

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46
Supervisory authority

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

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

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

Article 47
Independence

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

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

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

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

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

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

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

Article 48
General conditions for the members of the supervisory authority

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

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

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

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

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

Article 49

Rules on the establishment of the supervisory authority

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

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

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

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

(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

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

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

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

Article 50
Professional secrecy

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

SECTION 2
DUTIES AND POWERS

Article 51
Competence

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

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

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

Article 52
Duties

1. The supervisory authority shall:

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

   (b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;

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

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

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

(g) authorise and be consulted on the processing operations referred to in Article 34;

(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);

(i) approve binding corporate rules pursuant to Article 43;

(j) participate in the activities of the European Data Protection Board.

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

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

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

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

6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

Article 53
Powers

1. Each supervisory authority shall have the power:

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

   (b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;

   (c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;

   (d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;

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

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

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

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

   (i) to issue opinions on any issue related to the protection of personal data;

   (j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.

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

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

   (b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.

   The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.

3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

Article 54
Activity report

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

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 55
Mutual assistance

1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.

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

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

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

(b) compliance with the request would be incompatible with the provisions of this Regulation.

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

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

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

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

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

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

Article 56
Joint operations of supervisory authorities

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.

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

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

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

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

SECTION 2
CONSISTENCY

Article 57
Consistency mechanism

For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.

Article 58
Opinion by the European Data Protection Board

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

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

   (a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or

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

   (c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or

   (d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

   (e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

   (f) aims to approve binding corporate rules within the meaning of Article 43.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

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

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.

8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Article 59
Opinion by the Commission

1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.

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

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

4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Article 60
Suspension of a draft measure

1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:

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

   (b) adopt a measure pursuant to point (a) of Article 62(1).

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

3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.

Article 61
Urgency procedure

1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

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

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

4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62
Implementing acts

1. The Commission may adopt implementing acts for:

   (a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;

   (b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;

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

   (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

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

3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.

Article 63
Enforcement

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

2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64
European Data Protection Board

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

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

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

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

Article 65
Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

Article 66
Tasks of the European Data Protection Board

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

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

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

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

   (d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;

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

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

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

2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

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

Article 67
Reports

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

   The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

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

Article 68
Procedure

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

2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

Article 69
Chair

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

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.

Article 70
Tasks of the chair

1. The chair shall have the following tasks:

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

   (b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

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

Article 71
Secretariat

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

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

3. The secretariat shall be responsible in particular for:

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

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

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

   (d) the translation of relevant information;

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

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

Article 72
Confidentiality

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

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

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

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

Article 73
Right to lodge a complaint with a supervisory authority

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

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

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

Article 74

Right to a judicial remedy against a supervisory authority

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

2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.

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

Article 75

Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

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

Article 76
Common rules for court proceedings

1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.

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

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

4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.

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

Article 77
Right to compensation and liability

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

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

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

Article 78
Penalties

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

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

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

Article 79
Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.

3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:

   (k) a natural person is processing personal data without a commercial interest; or

   (l) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.

4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

   (m) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);

(n) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(o) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;

(p) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;

(q) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;

(r) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;

(s) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;

(t) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);

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

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

(v) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;

(w) processes special categories of data in violation of Articles 9 and 81;

(x) does not comply with an objection or the requirement pursuant to Article 19;

(y) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;

(z) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

(aa) does not designate a representative pursuant to Article 25;

(bb) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;

(cc) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;

(dd) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;

(ee) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;

(ff) misuses a data protection seal or mark in the meaning of Article 39;

(gg) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;

(hh) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);

(ii) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);

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

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

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80
Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

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

Article 80a
Processing of national identification number

Member States may determine the conditions for the processing of a national identification number or any other identifier of general application. [148]

Article 81
Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

[148] BE suggestion based on Article 8(7) of the 1995 Directive.

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

(b) 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, inter alia for medicinal products or medical devices; or

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

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 82

Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

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

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

Article 83

Processing for historical, statistical and scientific (…) purposes

1. (…) Personal data may be processed for historical, statistical or scientific (…) purposes only if:

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

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

2. Personal data processed for historical, statistical or scientific (…) purposes may be published or otherwise publicly disclosed (…) only if:

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

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

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

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

Article 84

Obligations of secrecy

1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

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

Article 85

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86
Exercise of the delegation

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

2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Article 87
Committee procedure

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

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

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

CHAPTER XI
FINAL PROVISIONS

Article 88
Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 89
Relationship to and amendment of Directive 2002/58/EC

1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2 Article 1(2) of Directive 2002/58/EC shall be deleted.

Article 90
Evaluation

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

Article 91
Entry into force and application

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

2. It shall apply from [*two years from the date referred to in paragraph 1*].

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

Done at Brussels,

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