INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE PROVIDED BY THE RAPPORTEUR
22 October 2013

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,

After consulting the European Data Protection Supervisor,

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.

(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[1] 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.

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

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

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

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. 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

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

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. 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.

(11) 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.

(12) 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.

(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, Regulation (EC) No 45/2001 should be brought in line with this Regulation and applied in accordance with this Regulation.

(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal, family-related, or domestic, such as correspondence and the holding of addresses or a private sale and without any connection with a professional or commercial activity. However, this Regulation should apply to controllers and processors which provide the means for processing personal data for such personal or domestic activities.

(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).

(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 public body may be disclosed by that authority or body in accordance with Union or Member State law regarding public access to official documents, which reconciles the right to data protection with the right of public access to official documents and constitutes a fair balance of the various interests involved.

(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.

(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, irrespective of whether connected to a payment or not, to such data subjects, or to the monitoring of such data subjects. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects residing in one or more Member States in the Union.

(21) In order to determine whether a processing activity can be considered to 'monitor' data subjects, it should be ascertained whether individuals are tracked, regardless of the origins of the data, or if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of data processing techniques which consist of applying a 'profile', particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(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 data protection should apply to any information concerning an 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 or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

(24) When using identifiers provided by devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers and Radio Frequency Identification tags, this Regulation should be applicable to processing involving such data, unless those identifiers do not relate to an identified or identifiable natural person.

(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 that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, . Clear affirmative action could include ticking a box when visiting an Internet website or 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, mere use of a service 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. Where data processing is based on the data subject's consent in relation to the offering of goods or services directly to a child, consent should be given or authorised by the child's parent or legal guardian in cases where the child is below the age of 13. Age-appropriate language should be used where the intended audience is children. Other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a 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. In case of a child or a person lacking legal capacity, relevant Union or Member State law should determine the conditions under which consent is given or authorised by that person.

(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. To comply with the principle of data minimisation, the burden of proof should not be understood as requiring the positive identification of data subjects unless necessary. Similar to civil law terms (Directive 93/13/EEC), data protection policies should be as clear and transparent as possible. They should not contain hidden or disadvantageous clauses. Consent can not be given for the processing of personal data of third persons.

(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. This is especially the case if the controller is a public authority that can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given. The use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent. Consent for the processing of additional personal data that are not necessary for the provision of a service should not be a required for using the service. When consent is withdrawn, this may allow the termination or non-execution of a service which is dependent on the data. Where the conclusion of the intended purpose is unclear, the controller should in regular intervals provide the data subject with information about the processing and request a re-affirmation of their consent.

(34) (deleted)

(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 which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. This should include also collective agreements that could be recognised under national law as having general validity. 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 the controller, or in case of disclosure, by the third party to whom the data is disclosed, may provide a legal basis for processing, provided that they meet the reasonable expectations of the data subject based on his or her relationship with the controller and 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. Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her relationship with the controller. The data subject should have the right to object the processing 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. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. 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 and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist accidental events 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 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. This principle also applies to processing of personal data to restrict abusive access to and use of publicly available network or information systems, such as the blacklisting of electronic identifiers.

(39a) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the prevention or limitation of damages on the side of the data controller should be presumed as carried out for the legitimate interest of the data controller or in case of disclosure, by the third party to whom the data is disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller. The same principle also applies to the enforcement of legal claims against a data subject, such as debt collection or civil damages and remedies.

(39b) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the processing of personal data for the purpose of direct marketing for own or similar products and services or for the purpose of postal direct marketing should be presumed as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data is disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller if highly visible information on the right to object and on the source of the personal data is given. The processing of business contact details should be generally regarded as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data is disclosed, and as meeting the reasonable expectations of the data

subject based on his or her relationship with the controller. The same should apply to the processing of personal data made manifestly public by the data subject.

(40) (deleted)
(41) (deleted)

(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, for historical, statistical and scientific research purposes, or for archive services.

(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. If it is possible for the data subject to provide such data, controllers should not be able to invoke a lack of information to refuse an access request.

(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 obtain, 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 reasonable 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 likely stored for each purpose, if the data are to be transferred to third parties or third countries, on the existence of measures to object and 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. This information should be provided, which can also mean made readily available, to the data subject after the provision of simplified information in the form of standardised icons.

(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 knows 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.

(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 estimated period, which recipients receive the data, what is the general logic of the data that are undergoing the processing and what might be the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, such as in relation to the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

(51a) 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. Data controllers should be encouraged to develop interoperable formats that enable

data portability. 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. Providers of information society services should not make the transfer of those data mandatory for the provision of their services.

(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 erasure 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. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research 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. Also, the right to erasure should not apply when the retention of personal data is necessary for the performance of a contract with the data subject, or when there is a legal obligation to retain this data.

(54) To strengthen the right to erasure 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 without legal justification should be obliged to take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation.

(54a) Data which are contested by the data subject and whose accuracy or inaccuracy cannot be determined should be blocked until the issue is cleared.

(55) (deleted)

(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, free of charge and in a manner that can be easily and effectively invoked. 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 the data subject has the right to object to the processing the controller should explicitly offer it to the data subject in an intelligible manner and form, using clear and plain language and should clearly distinguish it from other information.

(58) Without prejudice to the lawfulness of the data processing, every natural person should have the right to object to profiling. Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject should only 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. The In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human assessment and that such measure should not concern a child. Such measures should not lead to discrimination against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity.

(58a) Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.

(59) Restrictions on specific principles and on the rights of information, rectification and erasure or on the right of access and to obtain data, the right to object, 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 specific and well-defined 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 with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities. In particular, the controller should ensure and be able to demonstrate

the compliance of each processing operation with this Regulation. This should be verified by independent internal or external auditors.

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational 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. The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.

(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. The arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships. The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on their behalf.

(63) Where a controller not established in the Union is processing personal data of data subjects in the Union, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the processing relates to fewer than 5000 data subjects during any consecutive 12-month period and is not carried out on special categories of personal data, or is 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 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 be able to demonstrate compliance with this Regulation, the controller or processor should maintain the documentation necessary in order to fulfill the requirements laid down in this Regulation. 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 evaluating the compliance with this Regulation. However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.

(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, technological neutrality, interoperability and innovation should be promoted, and, where appropriate, cooperation with third countries should be encouraged.

(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 the controller should notify the breach to the supervisory authority without undue delay, which should be presumed to be not later than 72 hours. If applicable, 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.

(71a) Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited. Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with the regulation. Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable data management framework and by following it up with a comprehensive compliance mechanism.

(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) (deleted)

(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 data protection officer or 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 A consultation of the supervisory authority 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.

(74a) Impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them. Data controllers should therefore conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. It should further demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance.

(75) Where the processing is carried out in the public sector or where, in the private sector, processing relates to more than 5000 data subjects within 12 months, or where its core activities, regardless of the size of the enterprise, involve processing operations on sensitive data, or processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. When establishing whether data about a large number of data subjects are processed, archived data that is restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account. Such data protection officers, whether or not an employee of the controller and whether or not performing that task full time, should be in a position to perform their duties and tasks independently and enjoy special protection against dismissal. Final responsibility should stay with the management of an organization. The data protection officer should in particular be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.

(75a) The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.

(76) Associations or other bodies representing categories of controllers should be encouraged, after consultation of the representatives of the employees, 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. Such codes should make compliance with this Regulation easier for industry.

(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and standardised marks should be encouraged, allowing data subjects to quickly, reliably and verifiably assess the level of data protection of relevant products and services. A "European Data Protection Seal" should be established on the European level to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing non-European companies to more easily enter European markets by being certified.

(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 ensuring an adequate level of protection for the fundamental rights of citizens.

(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. The Commission may also decide, having given notice and a complete justification to the third country, to revoke such a decision.

(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. Any legislation which provides for extra-territorial access to personal data processed in the Union without authorisation under Union or Member State law should be considered as an indication of a lack of adequacy. 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. Those appropriate safeguards should uphold a respect of the data subject rights adequate to intra-EU processing, in particular relating to purpose limitation, right to access, rectification, erasure and to claim compensation. Those safeguards should in particular guarantee the observance of the principles of personal data processing, safeguard data subject rights and provide for effective redress mechanisms, ensure the observance of the principles of data protection by design and by default, guarantee the existence of a data protection officer.

(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 or supplementary safeguards 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. The standard data protection clauses adopted by the Commission could cover different situations, namely transfers from controllers established in the European Union to controllers established outside the European Union and from controllers established in the European Union to processors, including sub-processors, established outside the European Union. Controllers and processors should be

encouraged to provide even more robust safeguards via additional contractual commitments that supplement standard protection clauses.

(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 all 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, taking into full account the interests and fundamental rights of the data subject.

(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 for public health, or to competent public authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer 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 or another person's life, if the data subject is incapable of giving consent. Transferring personal data for such important grounds of public interest should only be used for occasional transfers. In each and every case, a careful assessment of all circumstances of the transfer should be carried out.

(88) For the purposes of processing for historical, statistical and scientific research 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 legally binding 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, to the extent that the processing is not massive, not repetitive and not structural. That guarantee should include financial indemnification in cases of loss or

unauthorised access or processing of the data and an obligation, regardless of national legislation, to provide full details of all access to the data by public authorities in the third country.

(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. In cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the EU on the one hand, and that of a third country on the other, the Commission should ensure that EU law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.

(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 on 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. An authority shall have adequate financial and personal resources to fully carry out its role, taking into account the size of the population and the amount of personal data processing.

(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 cooperation 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 appointed by the parliament or the government of the Member State taking due care to minimise the possibility of political interference, and include rules on the personal qualification of the members, the avoidance of conflicts of interest 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 act as the single contact point and the lead authority responsible for supervising 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 lead authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment or its representative. The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases on the request of a competent authority.

(98a) Data subjects whose personal data is processed by a data controller or processor in another Member State should be able to complain to the supervisory authority of their choice. The lead data protection authority should coordinate its work with that of the other authorities involved.

(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 or by an association acting in the public interest 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 or the association 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 of 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. Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion. 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.

(106a) In order to ensure the consistent application of this Regulation, the European Data Protection Board may in individual cases adopt a decision which is binding on the competent supervisory authorities.

(107) (deleted)

(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 European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the institutions of the Union and promoting cooperation of the supervisory authorities throughout the Union, including the coordination of joint operations. The European Data Protection Board should act independently when exercising its tasks. The European Data Protection Board should strengthen the dialogue with concerned stakeholders such as data subjects' associations, consumer organisations, data controllers and other relevant stakeholders and experts.

(111) Data subjects should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights 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 acts in the public interest and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority on behalf of data subjects with their consent or exercise the right to a judicial remedy if mandated by the data subject, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a breach of this Regulation 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 mandate any body, organisation or association acting in the public interest to bring 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. This does not apply to non-EU-residents. 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, in case of EU residence, where the data subject resides, unless the controller is a public authority of the Union or a Member State 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, whether pecuniary or not, 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 only 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. The rules on penalties should be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter of Fundamental Rights, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.

(119a) In applying penalties, Member States should show full respect for appropriate procedural safeguards, including the right to an effective judicial remedy, due process, and the principle of ne bis in idem.

(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) Whenever necessary, exemptions or derogations from the requirements of certain provisions of this Regulation for the processing of personal data should be provided for 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. 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, on co-operation and consistency, and on specific data processing situations. 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 broadly to cover all activities which aim at is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, also taking into account technological development. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

(122a) A professional who processes personal data concerning health should receive, if

possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the General Practitioner or to the Specialist who has requested such data processing.

(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.

(123a) The processing of personal data concerning health, as a special category of data, may be necessary for reasons of historical, statistical or scientific research. Therefore this Regulation foresees an exemption from the requirement of consent in cases of research that serves a high public interest.

(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment and the social security context. Member States should be able to regulate the processing of employees' personal data in the employment and the processing of personal data in the social security context, in accordance with the rules and minimum standards set out in this Regulation. Where a statutory basis is provided in the Member State in question for the regulation of employment matters by agreement between employee representatives and the management of the undertaking or the controlling undertaking of a group of undertakings (collective agreement) or under Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees, the processing of personal data in an employment context may also be regulated by such an agreement.

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

(125a) Personal data may also be processed subsequently by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest. Member State legislation should reconcile the right to the protection of personal data with the rules on archives and on public access to administrative information. Member States should encourage the drafting, in particular by the European Archives Group, of rules to guarantee

the confidentiality of data vis-à-vis third parties and the authenticity, integrity and proper conservation of data.

(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. The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.

(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, adequate 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 and recognised as compliant.

(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 standardised information policies; the right to erasure; codes of conduct; certification; transfers with an adequancy decision; transfers by the way of binding corporate rules; administrative sanctions; processing of personal data concerning health; minimum standards for processing data in the employment context. 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[2]. 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.

(132) (deleted)

(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

---

[2] 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.

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. Commission decisions and authorisations by supervisory authorities relating to transfers of personal data to third countries pursuant to Article 41(8) should remain in force for a transition period of five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.

(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[3].

(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[4].

(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

---

[3] OJ L 176, 10.7.1999, p. 36.

[4] OJ L 53, 27.2.2008, p. 52.

association with the implementation, application and development of the Schengen acquis[5].

(139) 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.

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 with regard to the processing of personal data and rules relating to the free movement of personal data.

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

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article 2
Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, irrespective of the method of processing, 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.

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

---

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

(a) in the course of an activity which falls outside the scope of Union law;

(b) (deleted)

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

(d) by a natural person in the course of an exclusively personal or household activity. This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons;

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

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.

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, whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects in the Union by a controller or processor not established in the Union, 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, to such data subjects in the Union; or

(b) the monitoring of such data subjects.

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.

Article 4
Definitions

For the purposes of this Regulation:

(1) (deleted)

(2) '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, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person;

(2a) 'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;

(2b) ‘encrypted data’ means personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access it;

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

(3a) 'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behaviour;

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

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

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

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

(7a) ‘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;

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

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

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

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

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

(13) 'main establishment' means the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. The following objective criteria may be considered among others: The location of the controller or processor's headquarters; the location of the entity within a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; the location where effective and real management activities are exercised determining the data processing through stable arrangements;

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, represents the controller with regard to the obligations of the controller under this Regulation;

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

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

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

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

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

CHAPTER II
PRINCIPLES

Article 5
Principles relating to personal data processing

Personal data shall be:

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

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation);

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data (data minimisation);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the

purposes for which they are processed, are erased or rectified without delay (accuracy).

(e) kept in a form which permits direct or indirect 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 solely for historical, statistical or scientific research or for archive purposes in accordance with the rules and conditions of Articles 83 and 83a and if a periodic review is carried out to assess the necessity to continue the storage, and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation);

(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);

(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity);

(f) processed under the responsibility and liability of the controller, who shall ensure and be able to demonstrate the compliance with the provisions of this Regulation (accountability).

Article 6
Lawfulness of processing

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

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

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

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

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

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

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

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

(a) Union law, or

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

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.

4. (deleted)

5. (deleted)

Article 7
Conditions for Consent

1. Where processing is based on consent, the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

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

data subject's consent which are partly in violation of this Regulation are fully void.

3. Notwithstanding other legal grounds for processing, 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. It shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.

4. Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b).

Article 8
Processing of personal data of a child

1. For the purposes of this Regulation, in relation to the offering of goods or services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or legal guardian. The controller shall make reasonable efforts to verify such consent, taking into consideration available technology without causing otherwise unnecessary processing of personal data.

1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.

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.

3. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices for the methods of verifying consent referred to in paragraph 1, in accordance with Article 66.

4. (deleted)

Article 9
Special categories of data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions, or related security measures shall be prohibited.

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 for one or more specified purposes, 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, or

   (aa) processing is necessary for the performance or execution 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;

   (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 or collective agreements providing for adequate safeguards for the fundamental rights and the interests of the data subject such as right to non-discrimination, subject to the conditions and safeguards referred to in Article 82; 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;

   (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; or

(g) processing is necessary for the performance of a task carried out for reasons of high public interest, on the basis of Union law, or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable measures to safeguard the fundamental rights and the interests of the data subject; or

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

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

(i a) processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a; or

(j) processing of data relating to administrative sanctions, judgments, criminal offences, 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 for the fundamental rights and the interests of the data subject. Any register of criminal convictions shall be kept only under the control of official authority.

3. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2, in accordance with Article 66.

Article 10
Processing not allowing identification

1. If the data processed by a controller do not permit the controller or processor to directly or indirectly identify a natural person, or consist only of pseudonymous data, the controller shall not process or acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data

controller is unable to comply with a request of the data subject, it shall inform the data subject accordingly.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY ANDMODALITIES

Article 10a
General principles for data subject rights

1. The basis of data protection is clear and unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Regulation aim to strengthen, clarify, guarantee and where appropriate, codify these rights.

2. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of his or her personal data, the right of access, rectification and erasure of their data, the right to obtain data, the right to object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.

Article 11
Transparent information and communication

1. The controller shall have concise, transparent, clear 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, in particular for any information addressed specifically to a child.

Article 12
Procedures and mechanisms for exercising the rights of the data subject

1. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically where possible.

2. The controller shall inform the data subject without undue delay and, at the latest within 40 calendar days 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 and, where possible, the data controller may provide remote access to a secure system which would provide the data subject with direct access to their personal data. Where the data subject makes the request in electronic form, the information shall be provided in electronic form where possible, unless otherwise requested by the data subject.

3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject of the reasons for the inaction 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 reasonable fee taking into account the administrative costs for providing the information or taking the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. (deleted)

6. (deleted)

Article 13
Notification requirement in the event of rectification and erasure

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 transferred, unless this proves impossible or involves a disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests this.

Article 13a
Standardised information policies

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14:

(a) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;

(b) whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;

(c) whether personal data are processed for purposes other than the purposes for which they were collected;

(d) whether personal data are disseminated to commercial third parties;
e) whether personal data are sold or rented out;

(f) whether personal data are retained in encrypted form.

2. The particulars referred to in paragraph 1 shall be presented pursuant to Annex X in an aligned tabular format, using text and symbols, in the following three columns:

(a) the first column depicts graphical forms symbolising those particulars;

(b) the second column contains essential information describing those particulars;

(c) the third column depicts graphical forms indicating whether a specific particular is met.

3. The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the consumers of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.

4. Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.

5. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying the particulars referred to in paragraph 1 and their presentation as referred to in paragraph 2 and in Annex 1.

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, after the particulars pursuant to Article 13a have been provided:

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

(b) the purposes of the processing for which the personal data are intended, as well as information regarding the security of the processing of personal data, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and where applicable, information on how they implement and meet the requirements of point f of Article 6(1);

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

(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 to object to the processing of such personal data, or to obtain 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 the data to a third country or international organisation and on the existence or absence of an adequacy decision by the Commission, or in case of transfers referred to in Article 42, Article 43, or point (h) of Article 44(1), reference to the appropriate safeguards and the means to obtain a copy of them;

(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;

(gb) meaningful information about the logic involved in any automated processing;

(h) any further information which is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk;

(ha) where applicable, information whether personal data was provided to public authorities during the last consecutive 12-month period.

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 mandatory or optional, as well as the possible consequences of failure to provide such data.

2a. In deciding on further information which is necessary to make the processing fair under 1(h), controllers shall have regard to any relevant guidance under Article 38.

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 specific personal data originate. If personal data originates from publicly available sources, a general indication may be given.

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 without undue delay where the above is not feasible; or

(aa) on request by a body, organization or association referred to in Article 73;

(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 transfer to another recipient is envisaged, and at the latest at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject; or

(bb) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity.

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 processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83, are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort and the controller has published the information for anyone to retrieve; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data; or

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

(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.

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

7. (deleted)

8. (deleted)

Article 15

Right to access and to obtain data for the data subject

1. Subject to Article 12(4), 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, and in clear and plain language, the following information:

(a) the purposes of the processing for each category of personal data;

(b) the categories of personal data concerned;

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

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

(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) (deleted)

(h) the significance and envisaged consequences of such processing;

(ha) meaningful information about the logic involved in any automated processing;

(hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.

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 an electronic and structured format, unless otherwise requested by the data subject. Without prejudice to Article 10, the controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.

2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under Article 5(1)(e).

2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of Article 14(5)(da) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.

3. (deleted)

4. (deleted)

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 providing a supplementary statement.

Article 17
Right 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, and to obtain from third parties the erasure of any links to, or copy or replication of that data, 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;

   (ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

   (d) the data has been unlawfully processed.

1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.

2. Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

3. The controller and, where applicable, the third party 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 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 in such a way that it is not subject to the normal data access and processing operations and can not be changed anymore, 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;

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be restricted;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with paragraphs 2a of Article 15;

(da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.

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. (deleted)

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

8a. 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.

9. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, 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
(deleted, content moved to Article 15(2b))

SECTION 4
RIGHT TO OBJECT AND PROFILING

Article 19
Right to object

1. The data subject shall have the right to object at any time to the processing of personal data which is based on points (d) and (e) 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 the processing of personal data is based on point (f) of Article 6(1), the data subject shall have at any time and without any further justification, the right to object free of charge in general or for any particular purpose to the processing of their personal data.

2a. The right referred to in paragraph 2 shall be explicitly offered to the data subject in an intelligible manner and form, using clear and plain language, in particular if addressed specifically to a child, and shall be clearly distinguishable from other information.

2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.

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 for the purposes determined in the objection.

Article 20
Profiling

1. Without prejudice to the provisions in Article 6 every natural person shall have the right to object to profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.

2. Subject to the other provisions of this Regulation, a person may be subjected to profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject only if the processing:

(a) is necessary for 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, provided that suitable measures to safeguard the data subject's legitimate interests have been adduced; 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;

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

3. Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures

which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.

4. (deleted)

5. Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.

5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) for further specifying the criteria and conditions for profiling pursuant to 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 in Articles 11 to 19 and Article 32, when such a restriction meets a clearly defined objective of public interest, respects the essence of the right to protection of personal data, is proportionate to the legitimate aim pursued and respects the fundamental rights and interests of the data subject and is 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) taxation matters;

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

(e) a monitoring, inspection or regulatory function in the framework of the exercise of a competent public 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 must be necessary and proportionate in a democratic society and shall contain specific provisions at least as to:

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

(b) the determination of the controller;

(c) the specific purposes and means of processing;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the right of data subjects to be informed about the restriction.

2a. Legislative measures referred to in paragraph 1 shall neither permit nor oblige private controllers to retain data additional to those strictly necessary for the original purpose.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22

Responsibility and accountability of the controller

1. The controller shall adopt appropriate policies and implement appropriate and demonstrable technical and organizational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with this Regulation, having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself.

1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.

2. (deleted)

3. The controller shall be able to demonstrate the adequacy and effectiveness of the measures referred to in paragraphs 1 and 2. Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.

3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct ass referred to in Article 38.

4. (deleted)

Article 23
Data protection by design and by default

1. Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, if any, shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate 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 with regard to the principles laid out in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.

1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to the Directive of the European Parliament and of the Council on

public procurement as well as according to the Directive of the European Parliament and of the Council on procurement by entities operating in the water, energy, transport and postal services sector (Utilities Directive).

2. The controller shall ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated 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 and that data subjects are able to control the distribution of their personal data.

3. (deleted)

4. (deleted)

Article 24
Joint controllers

Where several controllers jointly determines the purposes and means of the processing of personal data, 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. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.

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) a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems; or

(c) a public authority or body; or

(d) a controller only occasionally offering goods or services to data subjects in the Union, unless the processing of personal data concerns special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems.

3. The representative shall be established in one of those Member States where the offering of goods or services to the data subjects, or the monitoring of them, take place.

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 processing 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. The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that the processor shall:

(a) process personal data only on instructions from the controller, unless otherwise required by Union law or Member State law;

(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) determine the conditions for enlisting another processor only with the prior permission of the controller, unless otherwise determined.

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the appropriate and relevant 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, taking into account the nature of processing and the information available to the processor;

(g) return all results to the controller after the end of the processing, not process the personal data otherwise and delete existing copies unless Union or Member State law requires storage of the data;

(h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow on-site inspections;

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

3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.

4. If a processor processes personal data other than as instructed by the controller or becomes the determining party in relation to the purposes and means of data processing, 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. (deleted)

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 shall maintain regularly updated documentation necessary to fulfill the requirements laid down in this Regulation.

2. In addition, each controller and processor shall maintain documentation of 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;

(ba) the name and contact details of the controllers to whom personal data are disclosed, if any.

(c) (deleted)

(d) (deleted)

(e) (deleted)

(f) (deleted)

(g) (deleted)

(h) (deleted)

3. (deleted)
4. (deleted)
5. (deleted)
6. (deleted)

Article 29
Co-operation with the supervisory authority

1. The controller and, if any, 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, taking into account the results of a data protection impact assessment pursuant to Article 33, having regard to the state of the art and the costs of their implementation.

1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:

(a) the ability to ensure that the integrity of the personal data is validated;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;

(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;

(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;

(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.

2. The measures referred to in paragraph 1 shall at least:

(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

(b) protect personal data stored or transmitted against accidental or unlawful destruction, or accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and

(c) ensure the implementation of a security policy with respect to the processing of personal data.

3. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) for the technical and organizational 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.

4. (deleted)

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 notify the personal data breach to the supervisory authority.

2. The processor shall alert and inform the controller without undue delay 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 and mitigate its effects.

The information may if necessary be provided in phases.

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 be sufficient to enable the supervisory authority to verify

compliance with this Article and with Article 30. The documentation shall only include the information necessary for that purpose.

4a. The supervisory authority shall keep a public register of the types of breaches notified.

5. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) for establishing the data breach and determining the undue delay 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. (deleted)

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, the privacy, the rights or the legitimate interests 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 be comprehensive and use clear and plain language. It shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 31(3) and information about the rights of the data subject, including redress.

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 European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) as to the circumstances in which a personal data breach is likely to

adversely affect the personal data or the privacy, the rights or the legitimate interests of the data subject referred to in paragraph 1.

6. (deleted)

SECTION 3
LIFECYCLE DATA PROTECTION MANAGEMENT

Article 32a
Respect to Risk

1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.

2. The following processing operations are likely to present specific risks:

   (a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;

   (b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;

   (c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;

   (d) processing of personal data 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;

   (e) automated monitoring of publicly accessible areas on a large scale;

   (f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);

   (g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;

(h) 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;

(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.

3. According to the result of the risk analysis:

(a) where any of the processing operations referred to in paragraph 2 (a) or (b) exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;

(b) where any of the processing operations referred to in paragraph 2 (a), (b) or (h) exist, the controller shall designate a data protection officer in line with the requirements and exemptions laid down in Article 35;

(c) where any of the processing operations referred to in paragraph 2 (a), (b), (c), (d), (e), (f), (g) or (h) exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;

(d) where processing operations referred to in paragraph 2 (f) exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.

4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to paragraph 3 (c) the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall be documented.

Article 33
Data protection impact assessment

1. Where required pursuant to point c of Article 32a(3) 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 rights and freedoms of the data subjects, especially their right to protection of personal data. A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.

2. (deleted, content moved to Article 32a(2)))

3. The assessment shall have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall contain at least

(a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller,

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

(c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation,

(d) a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed,

(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;

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

(h) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;

(i) a list of the recipients or categories of recipients of the personal data;

(j) where applicable, a list of the intended 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;

(k) an assessment of the context of the data processing.

3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.

3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies.

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

Article 33a
Data protection compliance review

1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.

2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.

3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.

4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative, shall make the compliance review available, on request, to the supervisory authority.

5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.

Article 34
Prior consultation

1. (deleted)

2. The controller or processor acting on the controller's behalf shall consult the data protection officer, or in case a data protection officer has not been appointed, 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 data protection officer or 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 competent supervisory authority determines in accordance with its power 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 European Data Protection Board shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to paragraph 2.

6. The controller or processor shall provide the supervisory authority, on request, with the data protection impact assessment pursuant to 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.

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 a legal person and relates to more than 5000 data subjects in any consecutive 12-month period or

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

(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.

2. A group of undertakings may appoint a main responsible data protection officer, provided it is ensured that a data protection officer is easily accessible from each establishment.

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 four two years in case of an employee or two years in case of an external service contractor. 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. (deleted)

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 executive management of the controller or the processor. The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.

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

4. Data protection officers shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject.

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 raise awareness, to inform and advise the controller or the processor of their obligations pursuant to this Regulation, in particular with regard to technical and organisational measures and procedures, 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 consultation, if required pursuant Articles 32a, 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.;

(i) to verify the compliance with this Regulation under the prior consultation mechanism laid out in Article 34;

(j) to inform the employee representatives on data processing of the employees.

2. (deleted)

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 or the adoption of codes of conduct drawn up by a supervisory authority 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;

(aa) respect for consumer rights;

(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 shall without undue delay give an opinion in whether the processing under 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 or processors 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 shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 are in line with this Regulation and have general validity within the Union. This delegated act shall confer enforceable rights on data subjects.

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. (deleted)

1a. Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation, in

particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.

1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.

1c. The supervisory authorities and the European Data Protection Board shall cooperate under the consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.

1d. During the certification procedure, the supervisory authority may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf. Third party auditors shall have sufficiently qualified staff, be impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.

1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named "European Data Protection Seal".

1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.

1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.

1h. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the public.

2. (deleted)

2a. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.

3. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations, 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 1-1h, including requirements for accreditation of auditors, conditions for granting and

withdrawal, and requirements for recognition within the Union and in third countries. These delegated acts shall confer enforceable rights on data subjects.

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 specific 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 as well as the implementation of this legislation, the professional rules and security measures which are complied with in that country or by that international organisation, jurisprudential precedents, 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, including sufficient sanctioning powers, 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, in particular any legally binding conventions or instruments with respect to the protection of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 to 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. Such delegated acts shall provide for a sunset clause if they concern a processing sector and shall be revoked according to paragraph 5 as soon as an adequate level of protection according to this Regulation is no longer ensured.

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

4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the elements listed in paragraph 2 where a delegated act pursuant to paragraph 3 has been adopted.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 to decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure or no longer ensures 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.

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.

6a. Prior to adopting a delegated act pursuant to paragraphs 3 and 5, the Commission shall request the European Data Protection Board to provide an opinion on the adequacy of the level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.

7. The Commission shall publish in the Official Journal of the European Union and on its website 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 five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.

Article 42
Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, or decides that a third country, or a territory or processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5), a controller or processor may not transfer personal data to a third country, territory or an international organisation unless 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

   (aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39;

   (b) (deleted)

   (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, a "European Data Protection Seal" or binding corporate rules as referred to in points (a), (aa) or (c) of paragraph 2 shall not require any specific 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 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. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until two years after the entry into force of this Regulation unless amended, replaced or repealed by that supervisory authority before the end of this period.

Article 43
Transfers by way of binding corporate rules

1. The 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 group of undertakings and those external subcontractors that are covered by the scope of the binding corporate rules, and include their employees;

   (b) expressly confer enforceable rights on data subjects;

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

1a. With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding corporate rules pursuant to Article 43.

2. The binding corporate rules shall at least specify:

   (a) the structure and contact details of the group of undertakings and its members and those external subcontractors that are covered by the scope of the binding corporate rules;

   (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 minimisation, limited retention periods, data quality, data protection by design and by default, 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 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 format, procedures, criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, including transparency for data subjects, 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. (deleted)

Article 43a
Transfers or disclosures not authorised by Union law

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

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

3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with Article 44(1)(d) and (e) and (5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).

5. (deleted)

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) deleted

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. (deleted)

4. Points (b) and (c) 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.

7. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66

paragraph 1(b) for the purpose of further the criteria and requirements for data transfers on the basis 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 ensure 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;.

   (da) clarify and consult on jurisdictional conflicts with third countries.

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).

Article 45a
Report by the Commission

The Commission shall submit to the European Parliament and the Council at regular intervals, starting not later than four years after the date referred to in Article 91(1), a report on the application of Articles 40 to 45. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall be supplied without undue delay. The report shall be made public.

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, notwithstanding co-operation and consistency arrangements pursuant to Chapter VII of this Regulation.

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

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.

7a. Each Member State shall ensure that the supervisory authority shall be accountable to the national parliament for reasons of budgetary control.

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 fulfills 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 and in conformity with national legislation and practice, 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, whilst conducting their duties with independence and transparency as set out in the Regulation.

SECTION 2
DUTIES AND POWERS

Article 51
Competence

1. Each supervisory authority shall be competent to perform the duties and to exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State, without prejudice to Articles 73 and 74. Data processing by a public authority shall be supervised only by the supervisory authority of that Member State.

2. (deleted)

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 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 of specific and documented information received alleging unlawful processing 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;

(ja) certify controllers and processors pursuant to Article 39.

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 and on appropriate measures for personal data protection. Activities addressed specifically to children shall receive specific attention.

2a. Each supervisory authority shall together with the European Data Protection Board promote the awareness of controllers and processors on risks, rules, safeguards and rights in relation to the processing of personal data. This includes keeping a register of sanctions and breaches. The register should enroll both all warnings and sanctions as detailed as possible, and the resolving of breaches. Each supervisory authority shall provide micro, small and medium sized enterprise controllers and processors on request with general information on their responsibilities and obligations in accordance with this Regulation.

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 reasonable fee or not take the

action requested by the data subject. Such a fee shall not exceed the costs of taking the action requested. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

Article 53
Powers

1. Each supervisory authority shall, in line with this regulation, 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, or to order the controller to communicate a personal data breach to 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;

(ia) to certify controllers and processors pursuant to Article 39;

(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.

(ja) to put in place effective mechanisms to encourage confidential reporting of breaches of this Regulation, taking into account guidance issued by the European Data Protection Board pursuant to Article 66(4b).

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor without prior notice:

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

(b) access to any of its premises, including to any data processing equipment and means.

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 accordance with Article 79. This power shall be exercised in an effective, proportionate and dissuasive manner.

Article 54
Activity report

Each supervisory authority must draw up a report on its activities at least every two years. The report shall be presented to the respective 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 54a
Lead Authority

1. 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, or where personal data of the residents of several Member States are processed, the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible for the supervision of the processing activities of the controller or the processor in all Member States, in accordance with the provisions of Chapter VII of this Regulation.

2. The lead supervisory authority shall take appropriate measures for the supervision of the processing activities of the controller or processor for which it is responsible only after consulting all other competent supervisory authorities within the meaning of paragraph 1 of Article 51 in an endeavour to reach a consensus. For that purpose it shall in particular submit any relevant information and consult the other authorities before it adopts a measure intended to produce legal effects vis-à-vis a controller or a processor within the meaning of paragraph 1 of Article 51. The lead authority shall take the utmost account of the opinions of the authorities involved. The lead authority shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible.

3. The European Data Protection Board shall, at the request of a competent supervisory authority, issue an opinion on the identification of the lead authority responsible for a controller or processor, in cases where:

(a) it is unclear from the facts of the case where the main establishment of the controller or processor is located; or

(b) the competent authorities do not agree on which supervisory authority shall act as lead authority;

(c) the controller is not established in the Union, and residents of different Member States are affected by processing operations within the scope of this Regulation.

3a. Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall act as lead authority for the supervision of processing activities.

4. The European Data Protection Board may decide on the identification of the lead authority.

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 investigations and prompt information on the opening of cases and ensuing developments where the controller or processor has establishments in several Member States or where data subjects in several Member States are likely to be affected by processing operations. The lead authority as defined in Article 54a shall ensure the coordination with involved supervisory authorities and shall act as the single contact point for the controller or processor.

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 to the requesting supervisory authority 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. Where no definitive measure is yet possible because the assistance is not yet

completed, the requesting supervisory authority may take interim measures under Article 53 in the territory of its Member State.

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 in accordance with the procedure referred to in Article 57.

10. The European Data Protection Board 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.

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 the controller or processor has establishments in several Member States or 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 lead authority as defined in Article 54a shall involve the supervisory authority of each of those Member States 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. The lead authority shall act as the single contact point for the controller or processor.

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 both on matters of general scope and in individual cases in accordance with the provisions of this section.

Article 58
Consistency on matters of general application

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) (deleted)

   (b) (deleted)

   (c) (deleted)

   (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 of general application 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 of general application shall be dealt with in the consistency mechanism.

5. Supervisory authorities and the Commission shall without undue delay 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 without undue delay 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 secretariat of the European Data Protection Board shall provide translations of relevant information, where necessary.

6a. The European Data Protection Board shall adopt an opinion on matters referred to it under paragraph 2.

7. The European Data Protection Board may decide by simple majority whether to adopt an opinion on any the matter submitted under paragraphs 3 and 4 taking into account:

(a) whether the matter presents elements of novelty, taking account of legal or factual developments, in particular in information technology and in the light of the state of progress in the information society; and

(b) whether the European Data Protection Board has already issued an opinion on the same matter.

8. The European Data Protection Board shall adopt opinions pursuant to paragraphs 6a and 7 by a simple majority of its members. These opinions shall be made public.

Article 58a

Consistency in individual cases

1. Before taking a measure intended to produce legal effects within the meaning of Article 54a, the lead authority shall share all relevant information and submit the draft measure to all other competent authorities. The lead authority shall not adopt the measure if a competent authority has, within a period of three weeks, indicated it has serious objections to the measure.

2. Where a competent authority has indicated that it has serious objections to a draft measure of the lead authority, or where the lead authority does not submit a draft measure referred to in paragraph 1 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, the issue shall be considered by the European Data Protection Board.

3. The lead authority and/or other competent authorities involved and the Commission shall without undue delay electronically communicate to the European Data Protection Board using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, the grounds which make the enactment of such measure necessary, the objections raised against it and the views of other supervisory authorities concerned.

4. The European Data Protection Board shall consider the issue, taking into account the impact of the draft measure of the lead authority on the fundamental rights and freedoms of data subjects, and shall decide by simple majority of its members whether to issue an opinion on the matter within two weeks after the relevant information has been provided pursuant to paragraph 3.

5. In case the European Data Protection Board decides to issue an opinion, it shall do so within six weeks and make the opinion public.

6. The lead authority shall take utmost 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. Where the lead authority intends not to follow the opinion of the European Data Protection Board, it shall provide a reasoned justification.

7. In case the European Data Protection Board still objects to the measure of the supervisory authority as referred to in paragraph 5, it may within one month adopt by a two thirds majority a measure which shall be binding upon the supervisory authority.

Article 59
(deleted)

Article 60
(deleted)

Article 60a
Notification of Parliament and Council

The Commission shall notify the Council and the European Parliament at regular intervals, at least every two years, on the basis of a report from the Chair of the European Data Protection Board, of the matters dealt with under the consistency procedure, setting out the conclusions drawn by the Commission and the European Data Protection Board with a view to ensuring the consistent implementation and application of this regulation.

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 58a, 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. 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 of general application, after requesting an opinion of the European Data Protection Board, for:

   (a) (deleted)

   (b) deciding whether it declares draft standard data protection clauses referred to in point (d) of Article 42 (2), as having general validity;

   (c) (deleted)

   (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).

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) and (2) or adopts a measure despite an indication of serious objection pursuant to Article 58a(1), 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 European Parliament, Council or Commission, in particular:

   (a) advise the European Institutions 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 European Parliament, Council or 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, including on the use of enforcement powers;

(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;

(da) provide an opinion on which authority should be the lead authority pursuant to Article 54a(3);

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities, including the coordination of joint operations and other joint activities, where it so decides at the request of one or several 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.

(ga) give its opinion to the Commission in the preparation of delegated and implementing acts based on this Regulation;

(gb) give its opinion on codes of conduct drawn up at Union level pursuant to Article 38(4);

(gc) give its opinion on criteria and requirements for the data protection certification mechanisms pursuant to Article 39(9).

(gd) maintain a public electronic register on valid and invalid certificates pursuant to Article 39(8);

(ge) provide assistance to a national supervisory authorities, at their request;

(gf) establish and make public a list of the processing operations which are subject to prior consultation pursuant to Article 34;

(gg) maintain a registry of sanctions imposed on controllers or processors by the competent supervisory authorities.

2. Where the European Parliament, Council or 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 European Parliament, Council and 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.

4a. The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

4b. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with paragraph 1 (b) for establishing common procedures for receiving and investigating information concerning allegations of unlawful processing and for safeguarding confidentiality and sources of information received.

Article 67
Reports

1. The European Data Protection Board shall regularly and timely inform the European Parliament, Council and Commission about the outcome of its activities. It shall draw up a report at least every two years 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, unless otherwise provided in its rules of procedure.

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 at least two deputy chairpersons from amongst its members.

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

2a. The position of the chair shall be a full-time position.

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, legal, 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 may be confidential where necessary, unless otherwise provided in the rules of procedure. The agendas of the meetings of the Board shall be made public.

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 and the consistency mechanism, 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 acts in the public interest 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 breach of this regulation has occurred.

Article 74
Right to a judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, 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. Without prejudice to the consistency mechanism 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 of the Union or a Member State 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, 75 and 77 if mandated by 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, including non-pecuniary damage, as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to claim 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 of those controllers or processors shall be jointly and severally liable for the entire amount of the damage, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24.

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. The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive.

2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:

(a) a warning in writing in cases of first and non-intentional non-compliance;

(b) regular periodic data protection audits;

(c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.

2b. If the controller or the processor is in possession of a valid "European Data Protection Seal" pursuant to Article 39, a fine pursuant to paragraph 2a(c) shall only be imposed in cases of intentional or negligent incompliance.

2c. The administrative sanction shall take into account the following factors:

(a) the nature, gravity and duration of the incompliance,

(b) the intentional or negligent character of the infringement,

(c) the degree of responsibility of the natural or legal person and of previous breaches by this person,

(d) the repetitive nature of the infringement,

(e) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,

(f) the specific categories of personal data affected by the infringement,

(fa) the level of damage, including non-pecuniary damage, suffered by the data subjects,

(fb) the action taken by the controller or processor to mitigate the damage suffered by data subjects,

(fc) any financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement,

(g) the degree of technical and organisational measures and procedures implemented pursuant to:

(i) Article 23 - Data protection by design and by default

(ii) Article 30 - Security of processing

(iii) Article 33 - Data protection impact assessment

(iv) Article 33 a - Data protection compliance review

(v) Article 35 - Designation of the data protection officer

(ga) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53,

(gb) other aggravating or mitigating factors applicable to the circumstance of the case.

3. (deleted)

4. (deleted)

5. (deleted)

6. (deleted)

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the absolute amounts of the administrative fines referred to in paragraphs 2a, taking into account the criteria and factors referred to in paragraphs 2 and 2c.

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, on co-operation and consistency in Chapter VII and specific data processing situations in Chapter IX whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression in accordance with the Charter of Fundamental Rights of the European Union.

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
Access to documents

1. Personal data in documents held by a public authority or a public body may be disclosed by this authority or body in accordance with Union or Member State legislation regarding public access to official documents, which reconciles the right to the protection of personal data with the principle of public access to official documents.

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

Article 81
Processing of personal data concerning health

1. In accordance with the rules set out in this Regulation, in particular 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, consistent, and specific measures to safeguard the data subject's interests and fundamental rights, to the extent that these are necessary and proportionate, and of which the

effects shall be foreseeable by the data subject, for:

(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, and if the processing is carried out by a person bound by a confidentiality obligation; 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 and the provision of health services. Such processing of personal data concerning health for reasons of public interest shall not result in data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.

1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.

1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.

1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes shall be permitted only with the consent of the data subject, and shall be subject to the conditions and safeguards referred to in Article 83.

2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interests, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data

subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.

3. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying public interest in the area of public health as referred to in point (b) of paragraph 1 and high public interest in the area of research as referred to in paragraph 2a.

3a. 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 82

Minimum standards for processing data in the employment context

1. Member States may, in accordance with the rules set out in this Regulation, and taking into account the principle of proportionality, adopt by legal provisions specific rules regulating the processing of employees' personal data in the employment context, in particular for but not limited to the purposes of the recruitment and job applications within the group of undertakings, the performance of the contract of employment, including discharge of obligations, laid down by law and by collective agreements, in accordance with national law and practice, 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. Member States may allow for collective agreements to further specify the provisions set out in this Article.

1a. The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.

1b. Consent of an employee shall not provide a legal basis for the processing of data by the employer when the consent has not been given freely.

1c. Notwithstanding the other provisions of this Regulation, the legal provisions of Member States referred to in paragraph 1 shall include at least the following minimum standards:

(a) the processing of employee data without the employees' knowledge shall not be permitted. Notwithstanding sentence 1, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has

committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;

(b) the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances;

(c) where undertakings or authorities collect and process personal data in the context of medical examinations and/or aptitude tests, they must explain to the applicant or employee beforehand the purpose for which these data are being used, and ensure that afterwards they are provided with these data together with the results, and that they receive an explanation of their significance on request. Data collection for the purpose of genetic testing and analyses shall be prohibited as a matter of principle;

(d) whether and to what extent the use of telephone, e-mail, internet and other telecommunications services shall also be permitted for private use may be regulated by collective agreement. Where there is no regulation by collective agreement, the employer shall reach an agreement on this matter directly with the employee. In so far as private use is permitted, the processing of accumulated traffic data shall be permitted in particular to ensure data security, to ensure the proper operation of telecommunications networks and telecommunications services and for billing purposes.
Notwithstanding sentence 3, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;

(e) workers' personal data, especially sensitive data such as political orientation and membership of and activities in trade unions, may under no circumstances be used to put workers on so-called 'blacklists', and to vet or bar them from future employment. The processing, the use in the employment context, the drawing-up and passing-on of blacklists of employees or other forms of discrimination shall be prohibited. Member

States shall conduct checks and adopt adequate sanctions in accordance with Article 79(6) to ensure effective implementation of this point.

1d. Transmission and processing of personal employee data between legally independent undertakings within a group of undertakings and with professionals providing legal and tax advice shall be permitted, providing it is relevant to the operation of the business and is used for the conduct of specific operations or administrative procedures and is not contrary to the interests and fundamental rights of the person concerned which are worthy of protection. Where employee data are transmitted to a third country and/or to an international organization, Chapter V shall apply.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraphs 1 and 1b, 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, after requesting an opinion from the European Data Protection Board, 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 82a

Processing in the social security context

1. Member States may, in accordance with the rules set out in this Regulation, adopt specific legislative rules particularising the conditions for the processing of personal data by their public and private institutions and departments in the social security context if carried out in the public interest.

2. Each Member State shall notify to the Commission those provisions which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and any subsequent amendment affecting them.

Article 83

Processing for historical, statistical and scientific research purposes

1. In accordance with the rules set out in this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

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

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.

2. (deleted)

3. (deleted)

Article 83a
Processing of personal data by archive services

1. Once the initial processing for which they were collected has been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object.

2. Each Member State shall notify to the Commission 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 84
Obligations of secrecy

1. In accordance with the rules set out in this Regulation, Member States shall ensure specific rules are in place setting set out the powers by the supervisory authorities laid down in Article 53 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, adequate 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 adequate rules in accordance with paragraph 1 shall obtain a compliance opinion pursuant to Article 38.

Article 85a

Respect of fundamental rights

This Regulation shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the TEU.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 85b

Standard Forms

The Commission may, taking into account the specific features and necessities of various sectors and data processing situations, lay down standard forms for

(a) specific methods to obtain verifiable consent referred to in Article 8(1),

(b) the communication referred to in Article 12(2), including the electronic format,

(c) providing the information referred to in paragraphs 1 to 3 of Article 14,

(d) requesting and granting access to the information referred to in Article 15(1), including for communicating the personal data to the data subject,

(e) documentation referred to in paragraph 1 of Article 28,

(f) breach notifications pursuant to Article 31 to the supervisory authority and the documentation referred to in Article 31(4),

(g) prior consultations referred to in Article 34, and for informing the supervisory authorities pursuant to Article 34(6).

2. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.

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

Article 86
Exercise of the delegation

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

2. The delegation of power referred to in [Articles XXX] shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in [Articles XXX] 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 [Articles XXX] shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of six 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 six 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. (deleted)

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. Articles 1(2), 4 and 15 of Directive 2002/58/EC shall be deleted.

2a. The Commission shall present, without delay and by the date referred to in Article 91(2) at the latest, a proposal for the revision of the legal framework for the processing of personal data and the protection of privacy in electronic communications, in order to align the law with this regulation and ensure consistent and uniform legal provisions on the fundamental right to protection of personal data in the European Union.

Article 89a

Relationship to and amendment of Regulation (EC) 2001/45

1. The rules set out in this Regulation shall be applied to the processing of personal data by Union institutions, bodies, offices and agencies in relation to matters for which they are not subject to additional rules set out in Regulation (EC) 2001/45.

2. The Commission shall present, without delay and by the date specified in Article 91(2) at the latest, a proposal for the revision of the legal framework applicable to the processing of personal data by the Union institutions, bodies, offices and agencies.

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

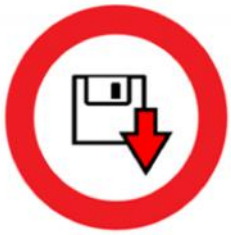
1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

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.

Annex 1 - Presentation of the particulars referred to in Article 13a

1. Having regard to the proportions referred to in point 6, particulars shall be provided as follows:

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

2. The following words in the rows in the second column of the table in point 1, entitled "ESSENTIAL INFORMATION", shall be formatted as bold:

(a) the word "collected" in the first row of the second column;

(b) the word "retained" in the second row of the second column;

(c) the word "processed" in the third row of the second column;

(d) the word "sold and rented out" in the fifth row of the second column;

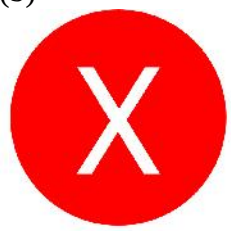
(e) the word "disseminated" in the fourth row of the second column;

(f) the word "unencrypted" in the sixth row of the second column.

3. Having regard to the proportions referred to in point 6, the rows in the third column of the table in point 1, entitled "FULFILLED", shall be completed with one of the following two graphical forms in accordance with the conditions laid down under point 4:

(a)

(b)



4.

(a) If no personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(b) If personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

(c) If no personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(d) If personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

(e) If no personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(f) If personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

(g) If no personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(h) If personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

(i) If no personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(j) If personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

(k) If no personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

(l) If personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

5. The reference colours of the graphical forms in point 1 in Pantone are Black Pantone No 7547 and Red Pantone No 485. The reference colour of the graphical

form in point 3a in Pantone is Green Pantone No 370. The reference colour of the graphical form in point 3b in Pantone is Red Pantone No 485.

6. *The proportions given in the following graduated drawing shall be respected, even where the table is reduced or enlarged:*