



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 31 May 2013

**Interinstitutional File:
2012/0011 (COD)**

**10227/13
ADD 1**

**DATAPROTECT 72
JAI 438
MI 469
DRS 104
DAPIX 86
FREMP 77
COMIX 339
CODEC 1257**

ADDENDUM TO NOTE

from:	Presidency
to:	Council
No. prev. doc.:	9398/1/13 REV 1 DATAPROTECT 61 JAI 355 MI 383 DRS 96 DAPIX 80 FREMP 53 COMIX 276 CODEC 1033 + REV 1 ADD 1
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Key issues of Chapters I-IV

All changes made to the original Commission proposal are underlined text, or, where text has been deleted, indicated by (...).

Where existing text has been moved, this text is indicated in italics.

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE
COUNCIL**

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN
UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee¹,

After consulting the European Data Protection Supervisor²,

Acting in accordance with the ordinary legislative procedure,

¹ OJ C, p. . .

² OJ C p. .

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 (...) 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 data³ 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.

³ OJ L 281, 23.11.1995, p. 31.

- 3a) (...) The right to the protection of personal data is not an absolute right; it 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.
- 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 (...) public and private individuals and undertakings across the Union has 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 should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

- 6) These developments require the construction of a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating 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 a consistent and high level of protection of individuals and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

- 9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.
- 10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.
- 11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

- 12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any such person. This should also apply where the name of the legal person contains the names of one or more natural persons.
- 13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.
- 14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union (...) nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
- 14a) (...) Regulation (EC) No 45/2001⁴ (...) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation (...).

⁴ OJ L 8, 12.1.2001, p. 1.

- 15) This Regulation should not apply to processing of personal data by a natural person in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities. However, this Regulation should (...) apply to controllers or 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, and, for these purposes, the maintenance of public order, 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/YYYY).
- When processing of personal data by (...) private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

- 16a) While this Regulation applies also to the activities of courts and other judicial authorities, Union or Member State law could, within the limits of this Regulation, specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. 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.
- 17) Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation. This Regulation should therefore 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. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body may be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile the interest of public access to official documents with the right to the protection of personal data.
- 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 to such data subjects irrespective of whether connected to a payment or not, or to the monitoring of the behaviour of such data subjects, which takes place in the Union. 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 doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union, or to the monitoring of the behaviour of such data subjects.
- 21) The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union. In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'

- 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 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 information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes. The principles of data protection should not apply to deceased persons.
- 24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not (...) be considered as personal data (...) if they do not identify an individual or make an individual identifiable.

- 25) Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, oral or electronic statement or by a clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This 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 or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing 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.
- 25a) Genetic data should be defined as 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, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.

- 26) Personal data relating to health should include in particular (...) data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services (...); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (...) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (...) or any information on for example 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 for example 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 not 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. (...).

- 30) Any processing of personal data should be lawful and fair. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them.

Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. 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 and relevant (...) 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. (...).

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. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.

- 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 legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- 32) Where processing is based on the data subject's consent, the controller should be able to demonstrate 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 the extent to which, consent is given.
- 33) For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.
- 34) In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. (...)
- 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 (...) basis in Union law or in the national law of a Member State. (...) It should be also for Union or national law to determine the purpose of the processing . Furthermore, this (...) basis could, within the limits of this Regulation, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be 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 authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.
- 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 or that of another person.

- 38) The legitimate interests of a controller including of a controller to which the data may be disclosed may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for Union or national law to provide (...) the (...) basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the exercise of their public duties.
- 39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. 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.

The processing of personal data to the extent strictly necessary for the purposes of preventing and monitoring fraud also constitutes a legitimate interest of the data controller concerned. A legitimate interest of a controller could include the processing of personal data for the purposes of anonymising or pseudonymising personal data. The processing of personal data for direct marketing purposes can be regarded as carried out for a legitimate interest.

- 40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific (...) purposes. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the consequences of the intended further processing for data subjects, and appropriate safeguards. Where the intended other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured. Further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

- 41) Personal data which are, by their nature, particularly sensitive (...) in relation to fundamental rights and freedoms, deserve specific protection. This should also include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless the data subject gives his or her explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.
- 42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where important grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific (...) purposes. A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.
- 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, for example by processing pseudonymous data, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. (...) However, the controller should not refuse to take information provided by the data subject supporting the exercise of his or her rights.
- 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 information could be provided in electronic form, for example, when addressed to the public, through a website. 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 (...) to a child, should be in such a clear and plain language that the child can easily understand.

- 47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, (...) in particular access to data, rectification, erasure and to exercise the right to object. Thus the controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons where the controller does not intend to comply with the data subject's request.
- 48) The principles of fair and transparent processing require that the data subject should be informed (...) of the existence of the processing operation and its purposes (...). The controller should provide the data subject with any further information necessary to guarantee fair and transparent processing. Furthermore the data subject should be informed about the existence of profiling, and the consequences of such profiling. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.
- 49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner.

- 50) However, it is not necessary to impose this obligation where the data subject already possesses this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific (...) purposes; in this regard, the number of data subjects, the age of the data, and any appropriate safeguards adopted may be taken into consideration.
- 51) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of 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, where possible for what period, which recipients receive the data, what is the logic involved in any automatic data processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates.
- 52) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. (...) A controller should not retain personal data for the sole purpose of being able to react to potential requests.

- 53) A natural person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is in particular relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific (...) purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.
- 54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take (...) reasonable steps, taking into account available technology and the means available to the controller, including technical measures, in relation to data for the publication of which the controller is responsible. (...)

- 54a) Methods to restrict processing of personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data unavailable to users or temporarily removing published data from a website. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted.
- 55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application (...) into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. The right to transmit the data into another automated processing system should not imply the erasure of personal data which have been provided by the data subject for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. By its very nature this right cannot be exercised against controllers processing data in the exercise of their public duties.
- 56) In cases where personal data might lawfully be processed (...) on grounds of (...) the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. It should be for the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

- 57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.
- 58) Every data subject should have the right not to be subject to a decision which is based on profiling (...). However, such profiling should be allowed when expressly authorised by Union or Member State law, including for fraud monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or carried out in the course of entering or performance of a contract between the data subject and a controller, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention (...). Profiling for direct marketing purposes or based on special categories of personal data should only be allowed under specific conditions.
- 59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

- 60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (...) be obliged to implement appropriate measures and be able to demonstrate the compliance of (...) processing activities with this Regulation, such as keeping a record, implementing technical and organisational measures for ensuring an appropriate level of security or performing a data protection impact assessment. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:
- *where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage; or*
 - where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
 - where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
 - where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;

- where personal data of vulnerable individuals, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

60a. Where the processing is likely to represent specific risks for the rights and freedoms of data subjects, the controller [or processor] should carry out, prior to the processing an assessment of the impact of the envisaged processing operations on the protection of personal data.

60b. *Where personal data are processed on behalf of the controller, the implementation of such measures should include in particular use only of a processor providing sufficient guarantees to implement appropriate technical and organisational measures.*

60c. Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the designation of a data protection officer or, where a data protection impact assessment indicates that processing operations involve a high degree of specific risks, through consultation of the supervisory authority prior to the processing.

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

- 62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes (...) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.
- 63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour 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 controller is a small or medium sized enterprise unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing or is a public authority or body (...). The representative should act on behalf of the controller and may be addressed by any supervisory authority.

The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance of the controller.

- 64) (...)
- (64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to present specific risks for the rights and freedoms of data subjects, the controller [or the processor] should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (...) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation.
- 65) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.
- 66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the specific risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, including confidentiality, taking into account available technology and the costs of (...) implementation in relation to the risks and the nature of the personal data to be protected. (...)

67) A personal data breach may, if not addressed in an adequate and timely manner, result in severe material or moral harm to individuals such as loss of control over their personal data or the limitation of their rights, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that (...). a personal data breach has occurred which may result in severe material or moral harm the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be severely 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 severely 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 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 (...) 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, the controller must ascertain whether all appropriate technological protection and organisational measures have been implemented 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.
- (68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data and using pseudonymous data.
- 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 obligations should be abolished, and replaced by effective procedures and mechanisms 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 (...) prior to the processing in order to assess the severity and likelihood of these specific risks, taking into account the nature, scope and purposes of the processing and the sources of the risks, 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 processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.
- 72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

- 73) Data protection impact assessments may be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.
- 74) Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their rights or giving rise to unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of the processing activities. The supervisory authority should **give advice** where the envisaged processing might not be in compliance with this Regulation. The supervisory authority should respond to the request for consultation in a defined period (...). However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its duties and powers laid down in this Regulation. Such consultation should equally take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing.

- 75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.
- 76) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risks inherent to the processing for the rights and freedoms of data subjects.
- 76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.
- 77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

121) Member States law should reconcile the rules governing freedom of expression, including journalistic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation, in particular as regards the general principles, the rights of the data subject, controller and processor obligations, the transfer of data to third countries or international organisations, the independent supervisory authorities and co-operation and consistency. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

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 (...) 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, 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:
 - (a) in the course of an activity which falls outside the scope of Union law (...);
 - (b) (...);
 - (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V the Treaty on European Union;
 - (d) by a natural person (...) in the course of (...) a personal or household activity;
 - (e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and, for these purposes, the maintenance of public order, or the execution of criminal penalties.
3. (...)

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

- (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.
- 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) '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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- (2a) 'pseudonymous data' means personal data processed in such a way that the data 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;

- (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 (...) or erasure;
- (3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
- (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 other than the data subject, the data controller or the data processor to which the personal data are disclosed; however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients;

- (8) 'the data subject's consent' means any freely-given, specific and informed (...) 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 a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question;
- (11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;
- (12) 'data concerning health' means data related to the physical or mental health of an individual, which reveal information about his or her health status;
- (12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to a natural person, in particular the analysis and prediction of aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;

- (13) ['main establishment' means
- as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, (...) the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place;.
 - as regards the processor, the place of its central administration in the European Union, and, if it has no central administration in the European Union, the place where the main processing activities take place;]
- (14) 'representative' means any natural or legal person established in the Union who, (...) designated by the controller in writing pursuant to Article 25, represents the controller with regard to the obligations of the controller under this Regulation (...);
- (15) 'enterprise' means any natural or legal person engaged in an economic activity, irrespective of its legal form, (...) including (...) 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) (...)

- (19) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 46;
- (20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services⁵.

⁵ OJ L 204, 21.7.1998, p. 37–48.

CHAPTER II

PRINCIPLES

Article 5

Principles relating to personal data processing

1. Personal data must be:
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (...);
 - (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;

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed (...) for historical, statistical or scientific (...) purposes pursuant to Article 83 (...);
 - (ee) processed in a manner that ensures appropriate security (...) of the personal data.
 - (f) (...)
2. The controller shall be responsible for compliance with paragraph 1.

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 unambiguous 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 by a controller to which the data are disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties.

(...)

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

- (a) Union law, or
- (b) national law of the Member State to which the controller is subject.

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Within the limits of this Regulation, the controller, processing operations and processing procedures, including measures to ensure lawful and fair processing, may be specified in this legal basis.

- 3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, inter alia:
- (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
 - (b) the context in which the data have been collected;
 - (c) the nature of the personal data;
 - (d) the possible consequences of the intended further processing for data subjects;
 - (e) the existence of appropriate safeguards.
4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1.
5. (...)

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous consent was given by the data subject.
- 1a. Where article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (...) from the other matters.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (...).
4. (...)

Article 8

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

1. Where Article 6 (1)(a) applies, in relation to the offering of information society 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 such consent is given or authorised by the child's parent or guardian.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the child's parent or guardian, taking into consideration available technology.

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

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

Article 9

Processing of special categories of personal data

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (...) shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data (...), 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
 - (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or
 - (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or
- (e) the processing relates to personal data which are manifestly made public by the data subject; or
- (f) processing is necessary for the establishment, exercise or defence of legal claims; or
- (g) processing is necessary for the performance of a task carried out for important reasons of public interest, on the basis of Union law or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or
- (h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or
- (i) processing is necessary for historical, statistical or scientific (...) purposes subject to the conditions and safeguards referred to in Article 83.
- (j) (...)

- 2a. *Processing of data relating to criminal convictions and offences or related security measures may only be carried out either under the control of official authority or when the processing is necessary for compliance with an (...) obligation to which a controller is subject, or for the performance of a task carried out for important reasons of public interest (...), and in so far as authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority.*
3. (...)

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (...) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (...) this Regulation..
2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 (...) do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.

CHAPTER III RIGHTS OF THE DATA SUBJECT

SECTION 1 TRANSPARENCY AND MODALITIES

Article 11

Transparent information and communication

1. (...)
2. (...)

Article 12

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

1. The controller shall take appropriate measures to provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or where appropriate, electronically or by other means.
- 1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 19. (...)

2. The controller shall provide the information referred to in Articles 14a and 15 and information on action taken on a request under Articles 16 to 19 to the data subject without undue delay and at the latest within one month of receipt of the request (...). This period may be extended for a further two months when necessary, taking into account the complexity of the request and the number of requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.
3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint to a supervisory authority (...).
4. Information provided under Articles 14 and 14a (...) and any communication under Articles 16 to 19 and 32 shall be provided free of charge. Where requests from a data subject are (...) manifestly unfounded or excessive, in particular because of their repetitive character, the controller (...) may refuse to act on the request. In that case, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
- 4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
5. (...)
6. (...)

Article 13
Rights in relation to recipients

(...)

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14

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

- 1.. Where personal data relating to a data subject are collected from the data subject, the controller shall (...), at the time when personal data are obtained, provide the data subject with the following information:
 - (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may also include the contact details of the data protection officer, if any;
 - (b) the purposes of the processing for which the personal data are intended (...);
- 1a. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed:
 - (a) (...);

- (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;
 - (c) the recipients or categories of recipients of the personal data;
 - (d) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation;
 - (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data (...);
 - (f) the right to lodge a complaint to a supervisory authority (...);
 - (g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data; and
 - (h) the existence of profiling referred to in Article 20(1) and (3) and information concerning (...) the profiling, as well as the significance and the envisaged consequences of such profiling of the data subject.*
2. (...)
 3. (...)
 4. (...)
 5. Paragraphs 1 and 1a shall not apply where and insofar as the data subject already has the information.

6. (...)
7. (...)
8. (...)

Article 14 a

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

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
 - (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may also include the contact details of the data protection officer, if any;
 - (b) the purposes of the processing for which the personal data are intended.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed (...):
 - (a) the categories of personal data concerned;
 - (b) (...)
 - (c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;

- (d) the recipients or categories of recipients of the personal data;
 - (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data (...);
 - (f) the right to lodge a complaint to a supervisory authority (...);
 - (g) the origin of the personal data, unless the data originate from publicly accessible sources;
 - (h) the existence of profiling referred to in Article 20(1) and (3) and information concerning (...) the profiling, as well as the significance and the envisaged consequences of such profiling of the data subject.*
3. The controller shall provide the information referred to in paragraphs 1 and 2:
- (a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or
 - (b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.
4. Paragraphs 1 to 3 shall not apply where and insofar as:
- (a) the data subject already has the information; or

- (b) the provision of such information in particular when processing personal data for historical, statistical or scientific purposes proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of such purposes; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests, for example by using pseudonymous data;
or
 - (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or
 - (d) where the data originate from publicly available sources; or
 - (e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person.
5. (...)
6. (...)

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge (...) confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed access to the data and the following information:

- (a) the purposes of the processing;
 - (b) (...)
 - (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries;
 - (d) where possible, the envisaged period for which the personal data will be stored;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
 - (f) the right to lodge a complaint to a supervisory authority (...);
 - (g) where the personal data are not collected from the data subject, any available information as to their source;
 - (h) in the case of decisions referred to in Article 20, knowledge of the logic involved in any automated data processing as well as the significance and envisaged consequences of such processing.
- 1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer.
- 1b. On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.

2. Where personal data supplied by the data subject are processed by automated means and in a structured and commonly used format, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject in that format to the data subject.
- 2a. The right to obtain a copy referred to in paragraphs 1b and 2 shall not apply where such copy cannot be provided without disclosing personal data of other data subjects
3. (...)
4. (...)
5. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met].

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification

1. (...) The data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (...) statement.
2. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.]

Article 17

Right to be forgotten and to erasure

1. The (...) controller shall have the obligation to erase personal data without undue delay and the data subject shall have the right to obtain the erasure of personal data without undue delay 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 point (a) of Article 9(2) and (...) 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(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2);
 - (d) the data have been unlawfully processed;
 - (e) the data have to be erased for compliance with a legal obligation to which the controller is subject.
2. (...)
- 2a. *Where the controller (...) has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take (...) reasonable steps, including technical measures, (...) to inform controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data.*
3. Paragraphs 1 and 2a shall not apply to the extent that (...) processing of the personal data is necessary:
- a. for exercising the right of freedom of expression in accordance with Article 80;

- b. *for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*;
 - c. for reasons of public interest in the area of public health in accordance with Article 81;
 - d. for historical, statistical and scientific (...) purposes in accordance with Article 83;
 - e. (...)
 - f. (...)
 - g. for the establishment, exercise or defence of legal claims.
4. (...)
5. (...)

Article 17a

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:
 - (a) the accuracy of the data 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 purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

- (c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. (...)
3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.
4. A data subject who obtained the restriction of processing pursuant to paragraph 1 (...) shall be informed by the controller before the restriction of processing is lifted.
5. (...)
- 5a. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.].

Article 17b

Notification obligation regarding rectification, erasure or restriction

The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

Article 18

Right to data portability

1. (...)
2. Where the data subject has provided personal data and the processing, (...) based on consent or on a contract, is carried on in an automated processing system provided by an information society service, the data subject shall have the right to withdraw these data in a form which permits the data subject to transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn.
- 2a. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights.
- [3. The Commission may specify (...) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]
4. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met .].

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19

Right to object

1. The data subject shall have the right to object, on reasoned grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (...) (f) of Article 6(1); the personal data shall no longer be processed unless the controller demonstrates (...) legitimate grounds for the processing which override the interests or (...) rights and freedoms of the data subject.
 - 1a. (...) Where an objection is upheld pursuant to paragraph 1 (...), the controller shall no longer (...) process the personal data concerned except for the establishment, exercise or defence of legal claims.
 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object (...) at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (...) and shall be presented clearly and separately from any other information.
 - 2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
3. (...)

4. [The rights provided for in this Article do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met].

Article 20

Profiling

1. Every data subject shall have the right not to be subject to a decision based solely on profiling which produces legal effects concerning him or her or severely affects him or her unless such processing:
 - (a) is carried out in the course of the entering into, or performance of, a contract between the data subject and a data controller and suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the rights of the data subject to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision or
 - (b) is (...) authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; or
 - (c) is based on the data subject's explicit consent (...).
2. (...)
3. Profiling shall not (...) be based on special categories of personal data referred to in Article 9(1), unless Article 9(2) applies and suitable measures to safeguard the data subject's legitimate interests are in place.
4. (...)
5. (...)

SECTION 5 RESTRICTIONS

Article 21

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 12 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:
 - (aa) national security;
 - (ab) defence;
 - (a) public security;
 - (b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, the maintenance of public order, or the execution of criminal penalties;
 - (c) other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters and the protection of market stability and integrity;
 - (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
 - (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

- (f) the protection of the data subject or the rights and freedoms of others.
2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the specification of the controller or categories of controllers and the applicable safeguards taking into account of the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects.

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1

GENERAL OBLIGATIONS

Article 22

Obligations of the controller

1. Taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller shall (...) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.
2. (...)
- 2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
- 2b. Compliance with the obligations of the controller may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39 (...).
3. (...)
4. (...)

Article 23

Data protection by design and by default

1. Having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall (...), implement (...) technical and organisational measures appropriate to the processing activity being carried on and its objectives, including the use of pseudonymous data, in such a way that the processing will meet the requirements of this Regulation and (...) protect the rights of (...) data subjects.
2. The controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are not excessive for each specific purpose of the processing are processed; this applies to the amount of (...) data collected, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.
- 2a. The controller may demonstrate compliance with the requirements set out in paragraphs 1 and 2 by means of a certification mechanism pursuant to Article 39.
3. (...)
4. (...)

Article 24

Joint controllers

1. (...) Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (...) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.
2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (...) controllers unless the data subject has been informed in a transparent manner which of the joint controllers is responsible.

Article 25

Representatives of controllers not established in the Union

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union.
2. This obligation shall not apply to:
 - (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

- (b) an enterprise employing fewer than 250 persons unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing; or
 - (c) a public authority or body.
 - (d) (...)
3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.
- 3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.
4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26

Processor

1. (...)The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (...) in such a way that the processing will meet the requirements of this Regulation (...)

- 1a. The provision of sufficient guarantees referred to in paragraph 1 may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39.
2. The carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
- (a) process the personal data only on instructions from the controller (...), unless required to do so by Union or Member State law to which the processor is subject and in such a case, the processor shall notify the controller unless the law prohibits such notification;
 - (b) (...)
 - (c) take all (...) measures required pursuant to Article 30;
 - (d) determine the conditions for enlisting another processor (...);
 - (e) as far as (...) possible, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;
 - (f) determine the extent to which the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34;
 - (g) return the personal data after the completion of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;

- (h) make available to the controller (...) all information necessary to demonstrate compliance with the obligations laid down in this Article.
- 3. The contract referred to in paragraph 2 shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.
- 4. (...)
- 5. (...)

Article 27

Processing under the authority of the controller and processor

(...)

Article 28

Records of categories of personal data processing activities

- 1. Each controller (...)and, if any, the controller's representative, shall maintain a record of all categories of personal data processing activities under its responsibility. This record shall contain (...) the following information:
 - (a) the name and contact details of the controller and any joint controller (...), controller's representative and data protection officer, if any;
 - (b) (...)
 - (c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f);

- (d) a description of categories of data subjects and of the categories of personal data relating to them;
 - (e) the (...) categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries;
 - (f) where applicable, the categories of transfers of personal data to a third country or an international organisation (...);
 - (g) where possible, the envisaged time limits for erasure of the different categories of data.
 - (h) (...)
- 2a. Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:
- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;
 - (b) the name and contact details of the data protection officer, if any;
 - (c) the categories of processing carried out on behalf of each controller;
 - (d) where applicable, the categories of transfers of personal data to a third country or an international organisation .
- 3a. The records referred to in paragraphs 1 and 2a shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.

3. On request, the controller and the processor and, if any, the controller's representative, shall make the record available (...) to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2a shall not apply to:
 - (a) (...)
 - (b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing; or
 - (c) categories of processing activities which by virtue of the nature, scope or purposes of the processing are unlikely to represent specific risks for the rights and freedoms of data subjects.
5. (...)
6. (...)

Article 29

Co-operation with the supervisory authority

(...)

SECTION 2

DATA SECURITY

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, including the use of pseudonymous data to ensure a level of security appropriate to these risks.
2. (...)
- 2a. The controller and processor may demonstrate compliance with the requirements set out in paragraph 1 by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39.
- 2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.
3. (...)
4. (...)

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.
- 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b).
2. (...) The processor shall alert and inform the controller without undue delay after becoming aware 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, where possible and appropriate, the categories and number of data subjects concerned and the categories and approximate 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) (...)
 - (d) describe the likely consequences of the personal data breach identified by the controller;

- (e) describe the measures taken or proposed to be taken by the controller to address the personal data breach; and
 - (f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.
- 3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.
4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. (...).
5. (...)
- [6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to severely affect the rights and freedoms of the data subject, the controller shall (...)communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (f) of Article 31(3).
3. The communication (...) to the data subject referred to in paragraph 1 shall not be required if:
 - a. the controller (...) has implemented appropriate technological protection measures and (...) those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption or the use of pseudonymous data; or
 - b. the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or
 - c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or
 - d. it would adversely affect a substantial public interest.
4. (...)
5. (...)
- [6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific risks for the rights and freedoms of data subjects, the controller (...) shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (...).
2. The following processing operations (...) present specific risks referred to in paragraph 1:
 - (a) a systematic and extensive evaluation (...) of personal aspects relating to (...) natural persons (...), which is based on profiling and on which decisions are based that produce legal effects concerning data subjects or severely affect data subjects;
 - (b) data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures, where the data are processed for taking (...) decisions regarding specific individuals on a large scale;
 - (c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (...);
 - (d) personal data in large scale processing systems containing genetic data or biometric data;

- (e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects.

- 2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

- 2b. Prior to the adoption of the list the supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union.

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

- 4. (...)

5. Where a controller is a public authority or body and where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6. (...)
7. (...)

Article 34

Prior (...) consultation

1. (...)
2. The controller (...) shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a high degree of specific risks.

(...)
3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller (...). This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.
4. (...)
5. (...)

6. When consulting the supervisory authority pursuant to paragraph 2, the controller (...) shall provide the supervisory authority, on request, with the data protection impact assessment provided for in Article 33 and any (...) information requested by the supervisory authority (...).
7. Member States shall consult the supervisory authority during the preparation of proposals for legislative or regulatory measures which provide for the processing of personal data and which may severely affect categories of data subjects by virtue of the nature, scope or purposes of such processing.
- 7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.
8. (...)
9. (...)

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller or the processor may, or where required by Union or Member State law shall, designate a data protection officer (...).
2. A group of undertakings may appoint a single data protection officer.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. (...)
5. The (...) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37 (...).
6. (...)
7. (...). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.
8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority (...).
10. Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.
11. (...)

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 the processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing (...) resources necessary to carry out these tasks as well as access to personal data and processing operations.
3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer (...) with the following tasks:
 - (a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation (...);
 - (b) to monitor compliance with this Regulation and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
 - (c) (...)
 - (d) (...)
 - (e) (...)
 - (f) (...)
 - (g) to monitor responses to requests from the supervisory authority and, within the sphere of the data protection officer's competence, to co-operate 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 of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter.
2. (...)

SECTION 5

CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.
- 1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:
 - (a) fair and transparent data processing;
 - (aa) the legitimate interests pursued by controllers in specific contexts;
 - (b) the collection of data;
 - (bb) the use of pseudonymous data;
 - (c) the information of the public and of data subjects;
 - (d) the exercise of the rights of data subjects;
 - (e) information and protection of children and the way to collect the parent's and guardian's consent;

- (ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security (...) of processing referred to in Article 30;
 - (ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;
 - (f) transfer of data to third countries or international organisations.
- 1b. Such a code of conduct shall contain mechanisms for monitoring and ensuring compliance with it by the controllers or processors which undertake to apply it, without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.
2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct, or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.
- 2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.
- 2b. Where the code of conduct relates to processing activities in several Member States, the supervisory authority shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which may give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.

3. Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, the European Data Protection Board shall submit its opinion to the Commission (...).
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).
5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 38a

Monitoring (...) of codes of conduct

1. Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 may be carried out by a (...) body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.
2. A body referred to in paragraph 1 may be accredited for this purpose if:
 - a. it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

- b. it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
 - c. it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;
 - d. it (...) demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.
- 3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.
- 4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.
- 5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.
- 6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Article 39

Certification

1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

(...)
2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.
3. The controller or processor which submits its processing to the certification mechanism shall provide the body referred to in Article 39a (1) with all information and access to its processing activities which are necessary to conduct the certification procedure. (...)
4. The certification issued to a controller or processor shall be subject to a periodic review by the body referred to in paragraph 1 of Article 39a or by the competent supervisory authority. It shall be withdrawn where the requirements for the certification are not or no longer met.

Article 39a

Certification body and procedure

1. Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, the certification and its periodic review may be carried out by a certification body which has an appropriate level of expertise in relation to data protection and is accredited by the supervisory authority which is competent according to Article 51.
2. The body referred to in paragraph 1 may be accredited for this purpose if:
 - a. it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
 - b. it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;
 - c. it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;
 - (d) it (...) demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.
3. *The supervisory authorities shall submit the draft criteria for the accreditation of the body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.*
4. The body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification, without prejudice to the responsibility of the controller or processor for compliance with this Regulation.

- 4a. Without prejudice to the provisions of Chapter VIII, the body referred to in paragraph 1 shall, subject to adequate safeguards, in cases of inappropriate use of the certification or where the requirements of the certification are not, or no longer, met by the controller or processor, withdraw the certification.
5. The body referred to in paragraph 1 shall provide the competent supervisory authority with the details of certifications issued and withdrawn and the reasons for withdrawing the certification.
6. The criteria for certification and the certification details shall be made public by the supervisory authority in an easily accessible form.
- 6a. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (...) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including conditions for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised ‘European Data Protection Seal’ within the Union and in third countries].
8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 80

Processing of personal data and freedom of expression

1. Member State law shall (...) reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression, including the processing of personal data for journalistic purposes and the purposes of artistic or literary expression.
2. (...)

Article 80a

Processing of personal data and public access to official documents

Personal data in official documents held by a public authority or a public body may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to such official documents with the right to the protection of personal data pursuant to this Regulation.
