COUNCIL OF THE EUROPEAN UNION

Brussels, 21 June 2013

11013/13

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 78
JAI 496
MI 546
DRS 119
DAPIX 88
FREMP 85
COMIX 380
CODEC 1475

NOTE

from:	Presidency
to:	Working Party on Information Exchange and Data Protection
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 DATAPROTECT 67 9967/13 JAI 418 MI 436 DRS 103DAPIX 85 FREMP 69 COMIX 330 CODEC 1175
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)

Delegations find attached a revised version of the draft General Data Protection Regulation. This version seeks to take account of the discussions on the draft Regulation that took place in the Working Party on Information Exchange and Data Protection. Only minor changes have been made to Articles 41 to 43 of Chapter V based on the discussions of 14 June 2013. With the exception of Articles 80 and 80a, the 4 December 2012 version of Chapter IX has not been amended.

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.

ANNEX

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 Committee[1],

After consulting the European Data Protection Supervisor[2],

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 data[3] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

3a) (…) 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.

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

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 45/2001[4] (…) applies to 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 (…).

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.

[4] OJ L 8, 12.1.2001, p. 1.

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/YYY).

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[5].

[5] DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. UK suggests deleting the words 'provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers' and 'received by the servers'. It also suggests deleting 'need not necessarily be considered as personal data in all circumstances ' and replacing it by 'can constitute personal data, but this will depend on the context'. COM referred to the ECJ case law (Scarlett C-70/10) according to which IP addresses should be considered as persona data if they actually could lead to the identification of data subjects. DE queried who would in practice be responsible for such metadata.

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 other 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 (…) and means of processing through stable arrangements. This criterion should not depend on 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 and, if it has no central administration in the Union, the place where the main processing activities take place in the Union.

Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

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. (…)[6].

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.

[6] COM reservation on deletion of the reference to the UN Convention on the Rights of the Child.

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 asses 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 provide 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.

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

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

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

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law.

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress.

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

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

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters or for public health, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent.

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

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

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

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

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

(92a) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subjected to control or monitoring mechanism regarding their financial expenditure[7].

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

94) Each supervisory authority should be provided with the (.) financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate annual budget, which may be part of the overall state or national budget.

[7] Presidency proposal in order to accommodate concerns raised by delegations that the wording of Article 47 would prevent this type of actions with regard to the supervisory authorities.

95) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State (…).

In order to ensure the independence of the supervisory authority, the member or members should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. They should behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

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

97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring those processing activities of the controller or processor throughout the Union and taking the related decisions as regards the controller or processor, in order to increase the consistent application, provide legal certainty and reduce the administrative burden for such controllers and processors. This should not apply in relation to controllers that are not established in the Union; their representative may be addressed by each supervisory authority, in addition to or instead of the controller.

The competence of the single supervisory authority should include measures intended to produce legal effects such as the authorisation of binding corporate rule and of transfers of personal data to third countries or international organisations, administrative fines and other sanctions. However, the competence of that supervisory authority should not encompass the competence for the enforcement of its decisions, on the territory of another Member State, unless in the context of joint operations and allowed by the Member State concerned.

98) The competent authority for the supervision of the processing and the related decisions, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment. However, the supervision of the processing by a public authority or body should be carried out solely by the supervisory authority or the supervisory authorities of the Member State where the public authority or body is established.

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

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

101) Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.
Where the supervisory authority to which the complaint has been lodged is not the competent supervisory authority, the competent supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases, the competent supervisory authority should, when taking measures intended to produce legal effects, including the imposition of penalties and administrative fines, take utmost account of the view of the supervisory authority to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

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

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

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

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

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

107) (…)

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

109) The application of this mechanism should be a condition for the (…) enforcement of the (…) decision by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, mutual assistance and joint operations might be carried out between the supervisory authorities *concerned* on a bilateral or multilateral basis without triggering the consistency mechanism.

110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

111) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence , and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.

112) Where a data subject considers that his or rights under this Regulation are infringed, he or she should have the right to mandate a body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects. Such a body, organisation or association should have the right to lodge, independently of a data subject's complaint, a complaint where it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.

113) Each natural or legal person should have the right to an effective judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

114) (…)

115) (…)

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

117) (…).

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

118a) In order to strengthen the enforcement of the rules of this Regulation, penalties and administrative fines may be imposed for any infringement of the Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. The imposition of penalties and administrative fines should be subject to adequate procedural safeguards in conformity with general principles of Union law and the Charter of Fundamental Rights, including effective judicial protection and due process.

119) Member States may lay down the rules on criminal sanctions for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. However, the imposition of criminal sanctions for infringements of such national rules and of administrative sanctions should not lead to the breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate offences, the upper limit and criteria for fixing the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the breach and of its consequences and the measures taken to ensure compliance with the obligations under the Regulation and to prevent or mitigate the consequences of the infringement. The consistency mechanism may also be used to promote a consistent application of administrative sanctions. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other sanctions under the Regulation.

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. (…)

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

123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

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

(124a) As regards statistics, Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities[8] provides further specifications on statistical confidentiality for European statistics.

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

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

[8] OJ L 87, 31.3.2009, p. 164–173.

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

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

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

130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers9. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

[9] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.

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

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

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

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

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

136) (…)

137) (…)

138) (…)[10.]

139) (…)[11]

[10] Recitals 136, 137 and 138 were deleted as this proposal is not Schengen relevant. COM scrutiny reservation on these deletions.

[11] Former recital 139 was moved up to recital 3a so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data[12].

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 <u>within the Union</u> shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.[13] [14].

---

12 DE scrutiny reservation: DE thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to internal market implications of the data processing operations.

13 DK, FR, NL, SI scrutiny reservation. FR thought that this paragraph, which was copied from the 1995 Data Protection Directive (1995 Directive 95/46), did not make sense in the context of a Regulation as this was directly applicable.

14 EE, FI, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. This is now regulated in Articles 80 and 80a of the draft Regulation.

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[15].

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[16], the maintenance of public order, or the execution of criminal penalties

3. (…).

---

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

16 BE reservation on the terms 'for these purposes'.

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[17].

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.

[17] UK reservation.

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[18] 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[19];

[18] UK is concerned that, together with recital 24, this will lead to risk-averse approach that this is always personal data.

[19] BE, DE, IT, SI, PL and PT scrutiny reservation. FR and UK reservation. FR and PL queried the need for a definition of pseudonymous data. UK thought the definition was too strict, making pseudonymous data tantamount to anonymous data

(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[20];

(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future[21];

(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[22;]

(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;

---

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

21 RO scrutiny reservation.

22 DE, FR SI, SK and UK scrutiny reservation. DE and SI thought this was completely outdated concept. COM explained that the definition had been taken over from Directive 95/46/EC and is related to the technical neutrality of the Regulation, as expressed in Article 2(1).

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; [23]

(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;[24] however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients[25];

(8) 'the data subject's consent' means any freely-given, specific and informed (…)[26] 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[27];

---

23 DE, DK, FR, LU and NL requested the inclusion of a definition of third party.

24 PT reservation. DE, FR, LU, NL, SI and SE regretted the deletion from the 1995 Data Protection Directive of the reference to third party disclosure and pleaded in favour of its reinstatement. COM argued that this reference was superfluous and that its deletion did not make a substantial difference.

25 DE, ES, NL and UK scrutiny reservation on latter part of definition. ES, NL and UK thought it could be deleted.

26 COM, CY, FR, GR, HU, IT, PL and RO reservation on the deletion of 'explicit'.

27 COM , supported by LU, explained that it sought to have a similar rule as in the E-Privacy Directive, which should be extended to all types of data processing. DE scrutiny reservation questioned the very broad scope of the duty of notifying data breaches, which so far under German law was limited to sensitive cases. NL, LV and PT concurred with DE and thought this could lead to over-notification. In the meantime the scope of Articles 31 and 32 has been limited.

(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[28];

(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[29] unique identification of that individual, such as facial images, or dactyloscopic data[30];

(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[31];

---

28 AT, CY, FR, IT, NL and SE scrutiny reservation. Several delegations (CH, CY, DE and SE) expressed their surprise regarding the breadth of this definition, which would also cover data about a person's physical appearance. DE thought the definition should differentiate between various types of genetic data. AT scrutiny reservation. The definition is now explained in the recital 25a.

29 ES preferred 'allows'; SI suggested 'allows or confirms'

30 NL, SE and AT scrutiny reservation. SI did not understand why genetic data were not included in the definition of biometric data. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. CH is of the opinion that the term 'biometric data' is too broadly defined.

31 CZ, DE, DK, EE, FR and SI expressed their surprise regarding the breadth of this definition. AT, BE, DE, NL, SI and LT scrutiny reservation. COM scrutiny reservation.

(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[32];

(13) 'main establishment' means

– as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes (…) and means of the processing of personal data are taken; if no decisions as to the purposes (…) 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[33];

– as regards the processor, the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place;[34]

[32] BE, RO and SE scrutiny reservation. BE, FR, LU, SI and RO would prefer reverting to the Council of Europe definition. COM reservation.

[33] BE, CZ DE, EE and SK scrutiny reservation: they expressed concerns about this definition, which might be difficult to apply in practice. DE thought it needed to be examined in conjunction with the one-stop-shop rules in Article 51. IE remarked this place may have no link with the place where the data are processed. DE also remarked that in the latter scenario, the Commission proposal did not determine which Member States' DPA would be competent. CZ thought the definition should be deleted.

[34] This definition will be revisited when discussing Chapter V.

Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking shall be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking;

(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[35];

(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[36];

(18) (…)[37]

35 DE scrutiny reservation. UK scrutiny reservation on all definitions in paragraphs 10 to 16.

36 DE wondered whether BCRs could also cover intra-EU data transfers.

37 COM scrutiny reservation on the deletion of the definition of a child.

(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 services[38] [39] [40].

[38] OJ L 204, 21.7.1998, p. 37–48.

[39] UK suggests adding a definition of 'competent authority' corresponding to that of the future Data Protection Directive.

[40] BE, DE; FR and RO suggest adding a definition of ‘transfer’ ('communication or availability of the data to one or several recipients'). RO suggests adding 'transfers of personal data to third countries or international organizations is a transmission of personal data object of processing or designated to be processed after transfer which ensure an adequate level of protection, whereas the adequacy of the level of protection afforded by a third country or international organization must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations'.

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[41];

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…)[42];

(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;

[41] This is without prejudice to later agreement on the regime for historical, statistical or scientific purposes in Article 83 and on the rules on further processing for incompatible purposes in Article 6(3a).

[42] COM reservation on the deletion of the data minimisation principle.

(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[43] (…);

(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[44]

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[45]consent to the processing of their personal data for one or more specific purposes[46];

(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;

43 This is without prejudice to later agreement on the regime for historical, statistical or scientific purposes in Article 83.

44 DE, AT, PT, SI and SK scrutiny reservation.

45 COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'

46 UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

(c) processing is necessary for compliance with a legal obligation to which the controller is subject[47];

(d) processing is necessary in order to protect the vital interests of the data subject **(…)**[48];

(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[49] [50];

(f) processing is necessary for the purposes of the legitimate interests[51] pursued by the controller or by a controller to which the data are disclosed [52] 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[53] [54].

---

47 HU thought that this subparagraph could be merged with 6(1) (e).

48 BG and ES scrutiny reservation; UK preferred the wording of the 1995 Directive.

49 COM clarified that this was the main basis for data processing in the public sector. DE, DK, LT and UK asked what was meant by 'public interest' whether the application of this subparagraph was limited to the public sector or could also be relied upon by the private sector. FR also requested clarifications as to the reasons for departing from the text of the 1995 Directive. UK suggested reverting to the wording used in Article 7(e) of the 1995 Directive.

50 The Presidency is of the opinion that subparagraphs (d) and (e) should be inverted.

51 FR and LT scrutiny reservation.

52 BG, CZ, DE, ES, HU, IT, NL, SE and UK asked to reinstate the words 'or by a third party' from the 1995 Directive. COM, supported by FR, thought that the use of the concept '*a* controller' should allow covering most cases of a third party.

53 ES and FR scrutiny reservation. BE, DK, SI, PT and UK had suggested deleting the last sentence.

54 DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified.

2. (…)

3. The basis for the processing referred to in points (c) and (e)[55] 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.[56]

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[57]:

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

---

55 FI and SI thought (f) should be added. BE, HU and FR thought (e) should be deleted. NL proposed adding a sentence: 'The purpose of the processing referred to in point (e) must be associated with the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

56 DK and DE scrutiny reservation; it was emphasised national law should not only have the possibility to specify, but also to enlarge the data protection rules of the Regulation.

57 DK, FI, NL, SI and SE stressed that the list should not be exhaustive. PT wanted to add consent by the data subject as an element.

(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[58].

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) [59] of paragraph 1[60].[61].[62]

5. (…).

58 BG, DE, ES and PL reservation: safeguards in themselves do not make further processing compatible.

59 FR and ES thought (f) should be added.

60 DE, HU, IT, NL and PT scrutiny reservation. IT and PT thought paragraph 4 could be deleted.

61 BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to in recital 40. BE, supported by FR, suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

62 HU thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here: 'Where personal data relating to the data subject are processed under this provision the controller shall inform the data subject according to Article 14 before the time of or within a reasonable period after the commencement of the first operation or set of operations performed upon the personal data for the purpose of further processing not compatible with the one for which the personal data have been collected.'

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous[63] 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. (…).

[63] COM reservation related to the deletion of 'explicit' in the definition of consent.

Article 8

Conditions applicable to child's consent in relation to information society services [64]

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child[65], the processing of personal data of a child below the age of 13 years[66] 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[67].

---

64 CZ, DE, AT, SE, SI, PT and UK scrutiny reservation. CZ and SI would prefer to see this Article deleted. NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. DE, supported by NO, opined this article could have been integrated into Article 7

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

66 Several delegations queried the expediency of setting the age of consent at 13 years: DE, FR, HU, LU, LV, RO and SI. DE, SI and RO proposed 14 years. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA).

67 DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law. SI thought the reference should be worded more broadly to 'civil law', thus encompassing also personality rights.

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(…)[68].

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)][69].

Article 9

***Processing of special categories of personal data*[70]**

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 (…)[71] shall be prohibited.[72]

---

68 ES, FR and SE scrutiny reservation.

69 LU reservation. ES, FR, SE and UK suggested deleting paragraphs 3 and 4.

70 SE, AT and NL scrutiny reservation. DE, supported by CZ, SE and UK, criticised on the concept of special categories of data, which does not cover all sensitive data processing operations. CZ, SE and UK pleaded in favour of a risk-based approach to sensitive data. The Presidency thought there was no majority in favour of such 'open' approach. SK and RO thought the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. SK also leaded in favour of the inclusion of national identifier.

71 The reference to criminal convictions and criminal offences has been deleted.

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

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 (…)[73], 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[74]; 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

---

73 Deleted at the suggestion of ES: the reference to Articles 7 and 8 was superfluous.

74 DE queried whether this paragraph obliged Member States to adopt specific laws on data protection regarding labour law relations; COM assured that the paragraph merely referred to a possibility to do so.

(e) the processing relates to personal data which are manifestly made public[75] by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims[76]; or

(g) processing is necessary for the performance of a task carried out <u>for *important*[77] reasons of</u> 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[78]; or

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

(j) (…)

---

75 DE, FR, SE and SI raised questions regarding the exact interpretation of the concept of manifestly made public (e.g. whether this also encompassed data implicitly made public and whether the test was an objective or a subjective one).

76 DE thought it should be clarified that also courts can process sensitive data.

77 ES, FR and UK scrutiny reservation on 'important'.

78 DE and EE scrutiny reservation. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.

2a. *Processing of data relating to criminal convictions and offences*[79] *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[80]. A complete register of criminal convictions may be kept only under the control of official authority[81].

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[82] in order to identify the data subject for the sole purpose of complying with (…) this Regulation.[83].

79 EE reservation: under its constitution all criminal convictions are mandatorily public.

80 NL scrutiny reservation. UK queried the relationship between this paragraph and Article 2(2) (c). COM argued that the reference to civil proceedings in Article 8(5) of the 1995 Directive need not be included here, as those proceedings are as such not sensitive data. DE and SE were not convinced by this argument.

81 SE scrutiny reservation. UK reservation on last sentence.

82 BE proposal, supported by ES.

83 AT, DE, FR, HU and UK scrutiny reservation.

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[84].

[84] DK, NL, SE and SI scrutiny reservation; COM reservation. BE thought this paragraph could also be moved to a recital.

CHAPTER III
RIGHTS OF THE DATA SUBJECT[85]

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[86]

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[87]. 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[88]. (…)

85 General scrutiny reservation by UK on the articles in this Chapter.
86 DE, SE, SI and FI scrutiny reservation.
87 COM reservation on deletion.
88 SI and UK thought this paragraph should be deleted.

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[89] (…). 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 (…)[90] *manifestly* unfounded or excessive, in particular because of their repetitive character, the controller (…) may refuse to act on[91] the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request[92].

---

89 UK pleaded in favour of deleting the one-month period. BG and PT thought it more simple to revert to the requirement of 'without excessive delay' under the 1995 Data Protection Directive.

90 LT and PL thought the criterion of 'manifestly excessive' required further clarification, e.g. through an additional recital. COM reservation on deletion.

91 NL scrutiny reservation: avoid that this gives the impression that public authority cannot refuse to consider request by citizen.

92 IT scrutiny reservation.

4a. Without prejudice to Article 10[93], 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[94].

5. (…)

6. (…)

Article 13

Rights in relation to recipients

(…)

93 ES proposal.
94 Further to UK proposal.

SECTION 2

INFORMATION AND ACCESS TO DATA

Article 14

Information to be provided where the data are collected from the data subject[95]

1[96]. 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 (…);

95 DE, EE, ES, NL, SE, FI, PT and UK scrutiny reservation. DE, supported by ES and NL, has asked the Commission to provide an assessment of the extra costs for the industry under this provision.

96 HU thought the legal basis of the processing should be included in the list.

1a. In addition to the information referred to in paragraph 1, the controller shall[97] provide the data subject with such further information [98]necessary to ensure fair and transparent processing in respect of the data subject[99], having regard to the specific circumstances and context in which the personal data are processed[100]:

(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[101];

(d) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation;

97 DE, EE, and PL asked to insert "on request". DE, DK, NL and UK doubted whether the redraft would allow for a sufficient risk-based approach and warned against excessive administrative burdens/compliance costs. DK and UK in particular referred to the difficulty for controllers in assessing what is required under para. 1a in order to ensure fair and transparent processing. DE, EE and PL pleaded for making the obligation to provide this information contingent upon a request thereto as the controller might otherwise take a risk-averse approach and provide all the information under Article 14(1a), also in cases where not required. UK thought that many of the aspects set out in paragraph 1a of Article 14 (and paragraph 2 of Article 14a) could be left to guidance under Article 39.

98 CZ suggested adding the word 'obviously'.

99 FR scrutiny reservation.

100 COM reservation on deletion of the words 'such as'.

101 AT and DE thought that this concept was too vague (does it e.g. encompass employees of the data controller?).

(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 **(…)**[102];

(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[103]; 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*.[104]

2. (…)[105]

3. (…)

4. (…)

5. Paragraphs 1 and 1a shall not apply where and insofar as the data subject already has the information.

6. (…)

7. (…)

8. (…)

---

102 The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE.

103 CZ, DE, ES and NL reservation.

104 SE scrutiny reservation. At the suggestion of PL the reference to 'logic' has been deleted.

105 HU reservation on the deletion of this paragraph.

Article 14 a

Information to be provided where the data have not been obtained from the data subject[106]

1[107]. 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[108] 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;

106 DE, EE, ES, NL (§§1+2),AT, PT scrutiny reservation.

107 HU thought the legal basis of the processing should be included in the list.

108 ES, IT and FR doubts on the addition of the words 'and context'.

(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[109];

(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.[110]

3. The controller shall provide the information referred to in paragraphs 1 and 2[111]:

(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.

109 COM and AT scrutiny reservation.

110 PL asks for the deletion of the reference to 'logic'.

111 BE proposed to add: 'possibly through an easily accessible contact person where the data subject concerned can consult his data'. This is already covered by the modified recital 46.

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[112] proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of such purposes;[113] in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[114], for example by using pseudonymous data[115]; 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[116]; or

(d) where the data originate from publicly available sources[117]; or

---

112 Text proposed by the Statistics Working Party in 10428/12, supported by FR, PL and UK. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into.

113 COM scrutiny reservation.

114 Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.

115 BE, FR and IT reservation on the mentioning of pseudonymous data.

116 UK thought the requirement of a legal obligation was enough and no further appropriate measures should be required.

117 COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.

(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[118].

5. (…)

6. (…)

Article 15

Right of access for the data subject[119]

1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge[120] (…) 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[121];

(b) (…)

118 COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.

119 DE, FI and SE scrutiny reservation. DE, LU and UK expressed concerns on overlaps between Articles 14 and 15.

120 DE, ES, HU, IT and PL reservation on the possibility to charge a fee. DE, LV and SE thought that free access once a year should be guaranteed.

121 HU thought the legal basis of the processing should be added.

(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[122];

(d) where possible, the envisaged[123] 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 (…)[124] [125];

(g) where the personal data are not collected from the data subject, any available information as to their source[126];

(h) in the case of decisions referred to in Article 20, knowledge of the logic involved[127] in any automated data processing as well as the significance and envisaged consequences of such processing[128].

---

122 UK reservation on the reference to recipients in third countries. IT thought the concept of recipient should be clarified, inter alia by clearly excluding employees of the controller.

123 ES and UK proposed adding 'where possible'; FR reservation on 'where possible ' and 'envisaged'; FR empahasised the need of providing an exception to archives.

124 DE thought it was too onerous to repeat this for every data subject and pointed to difficulties in ascertaining the competent DPA in its federal structure.

125 IT suggestion to delete subparagraphs (e) and (f) as under Article 14 this information should already be communicated to the data subject at the moment of the collection of the data.

126 SK scrutiny reservation: subparagraph (g) should be clarified.

127 PL reservation on the reference to 'logic': the underlying algorithm should not be disclosed. DE reservation on reference to decisions.

128 NL scrutiny reservation. CZ and FR likewise harboured doubts on its exact scope.

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[129] of the appropriate safeguards pursuant to Article 42 relating to the transfer[130].

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[131], provide a copy of the data concerning the data subject in that format to the data subject[132].

129 Further to CZ, ES and PL suggestion.

130 FR and UK scrutiny reservation on links with Chapter V

131 Further to ES suggestion.

132 COM, ES and FR reservation: they thought this was too narrowly drafted. DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy. DE scrutiny reservation on relation to paragraph 1.

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 [133]

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][134].

133 DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.

134 Text proposed by the Statistics Working Party in 10428/12. Supported by BE, CZ, FR and NL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into. BE suggested adding ' and the right of access is likely to render impossible or to seriously impair the achievement of such purposes '

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[135]

1. (…) The data subject shall have the right[136] 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.][137]

135 DE and UK scrutiny reservation.

136 UK suggested to insert the qualification ' where reasonably practicable' UK also suggested inserting the qualification 'where necessary'.

137 Text proposed by the Statistics Working Party in 10428/12. Supported by BE, FR and NL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will be looked into. BE, supported by PT, suggested adding ' and the right of access is likely to render impossible or to seriously impair the achievement of such purposes '

Article 17

Right to be forgotten and to erasure[138]

1. The (…) controller[139] shall have the obligation to erase personal data <u>without undue delay and the data subject shall have the right to obtain the erasure of personal data</u> <u>without undue delay</u> where one of the following grounds applies:

---

138 DE, EE, PT, SE, SI, FI and UK scrutiny reservation. EE, FR, NL, RO and SE reservation on the applicability to the public sector. Whereas some Member States have welcomed the proposal to introduce a right to be forgotten (AT, EE, FR, IE); other delegations were more sceptical as to the feasibility of introducing a right which would go beyond the right to obtain from the controller the erasure of one's own personal data (DE, DK, ES). The difficulties flowing from the household exception (UK), to apply such right to personal data posted on social media were highlighted (BE, DE, FR), but also the impossibility to apply such right to 'paper/offline' data was stressed (EE, LU, SI). Some delegations (DE, ES) also pointed to the possible externalities of such right when applied with fraudulent intent (e.g. when applying it to the financial sector). Several delegations referred to the challenge to make data subjects active in an online environment behave responsibly (DE, LU and UK) and queried whether the creation of such a right would not be counterproductive to the realisation of this challenge, by creating unreasonable expectations as to the possibilities of erasing data (DK, LU and UK). Some delegations thought that the right to be forgotten was rather an element of the right to privacy than part of data protection and should be balanced against the right to remember and access to information sources as part of the freedom of expression (DE, ES, LU, NL, SI, PT and UK). It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LV, LU, NL, SE and SI).

139 DE pointed to the difficulties in determining who is the controller in respect of data who are copied/made available by other controllers (e.g. a search engine) than the initial controller (e.g. a newspaper). AT opined that the exercise of the right to be forgotten would have take place in a gradual approach, first against the initial controller and subsequently against the 'secondary' controllers. ES referred to the problem of initial controllers that have disappeared and thought that in such cases the right to be forgotten could immediately be exercised against the 'secondary controllers' ES suggested adding in paragraph 2: ' Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof'. The Commission, however, replied that the right to be forgotten could not be exercised against journals exercising freedom of expression. According to the Commission, the indexation of personal data by search engines is a processing activity not protected by the freedom of expression.

(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[140];

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[141].

2. (…).

140 UK scrutiny reservation: this was overly broad.
141 RO scrutiny reservation.

2a. *Where the controller[142] (…) has made the personal data public[143]* <u>*and is obliged pursuant to paragraph 1 to erase the data*</u>, <u>the controller, taking account of available technology and the cost of implementation[144]</u>, *shall take (…) reasonable steps[145], including technical measures, (…) to inform* <u>*controllers[146]*</u> *which are processing* <u>the</u> *data, that a data subject requests them to erase any links to, or copy or replication of that personal data[147].*

---

142 BE, DE and SI queried whether this also covered controllers (e.g. a search engine) other than the initial controller (e.g. a newspaper).

143 ES prefers referring to 'expressly or tacitly allowing third parties access to'. IE thought it would be more realistic to oblige controllers to erase personal data which are under their control, or reasonably accessible to them in the ordinary course of business, i.e. within the control of those with whom they have contractual and business relations. BE, supported by IE and LU, also remarked that the E-Commerce Directive should be taken into account (e.g. through a reference in a recital) and asked whether this proposed liability did not violate the exemption for information society services provided in that Directive (Article 12 of Directive 2000/31/EC of 8 June 2000), but COM replied there was no contradiction. LU pointed to a risk of obliging controllers in an online context to monitor all data traffic, which would be contrary to the principle of data minimization and in breach with the prohibition in Article 15 of the E-Commerce Directive to monitor transmitted information.

144 Further to NL suggestion. The Presidency hopes this can also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;

145 LU queried why the reference to all reasonable steps had not been inserted in paragraph 1 as well and SE, supported by DK, suggested clarifying it in a recital. COM replied that paragraph 1 expressed a results obligation whereas paragraph 2 was only an obligation to use one's best efforts. ES thought the term should rather be 'proportionate steps'. DE, ES and BG questioned the scope of this term. ES queried whether there was a duty on controllers to act proactively with a view to possible exercise of the right to be forgotten. DE warned against the 'chilling effect' such obligation might have on the exercise of the freedom of expression.

146 BE, supported by ES and FR, suggested referring to 'known' controllers (or third parties).

147 BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule.

3. Paragraphs 1 and 2a shall not apply[148] 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[149];

b. for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject[150] or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[151];

c. for reasons of public interest in the area of public health in accordance with Article 81[152];

148 DE queried whether these exceptions also applied to the abstention from further dissemination of personal data. AT and DE pointed out that Article 6 contained an absolute obligation to erase data in the cases listed in that article and considered that it was therefore illogical to provide for exception in this paragraph.

149 DE and EE asked why this exception had not been extended to individuals using their own freedom of expression (e.g. an individual blogger).

150 In general DE thought it was a strange legal construct to lay down exceptions to EU obligations by reference to national law. DK and SI were also critical in this regard. UK thought there should be an exception for creditworthiness and credit scoring, which is needed to facilitate responsible lending, as well as for judicial proceedings. IT suggested inserting a reference to Article 21 (1).

151 AT scrutiny reservation.

152 DK queried whether this exception implied that a doctor could refuse to erase a patient's personal data notwithstanding an explicit request to that end from the latter. ES and DE indicated that this related to the more general question of how to resolve differences of view between the data subject and the data controller, especially in cases where the interests of third parties were at stake. PL asked what was the relation to Article 21.

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 17*a*

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[153];

(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.

[153] FR scrutiny reservation: FR thought the cases in which this could apply, should be specified.

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[154].

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[155].

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.][156].

154 DE , ES and SI asked who was to define the concept of public interest. DE reservation.

155 DE, PT, SI and IT thought that this paragraph should be a general obligation regarding processing, not limited to the exercise of the right to be forgotten. DK likewise thought the first sentence should be moved to Article 22.

156 Text proposed by the Statistics Working Party in 10428/12. Supported by ES and PL. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will be looked into. BE suggested adding ' and the right of access is likely to render impossible or to seriously impair the achievement of such purposes '

Article 17b

Notification obligation regarding rectification, erasure or restriction[157]

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[158] to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

157 Whilst several delegations agreed with this proposed draft and were of the opinion that it added nothing new to the existing obligations under the 1995 Directive, some delegations (DE, PL, SK and NL) pointed to the possibly far-reaching impact in view of the data multiplication since 1995, which made it necessary to clearly specify the exact obligations flowing from this proposed article. Thus, DE was opposed to a general obligation to log all the disclosures to recipients. DE also pointed out that the obligation should exclude cases where legitimate interests of the data subject would be harmed by a further communication to the recipients, that is not the case if the recipient would for the first time learn negative information about the data subject in which he has no justified interest. BE and ES asked that the concept of a 'disproportionate effort' be clarified in a recital.

158 BE, supported by ES and FR, suggested referring to 'known' recipients.

Article 18

Right to data portability[159]

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[160] provided by an information society service,[161] 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.

---

159 UK reservation: while it supports the concept of data portability in principle, the UK considers it not within scope of data protection, but in consumer or competition law. Several other delegations (DK, DE, FR, IE, NL, PL and SE) also wondered whether this was not rather a rule of competition law and/or intellectual property law or how it related to these fields of law. Therefore the UK thinks this article should be deleted. DE, DK and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to/raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, SE and UK pointed to the considerable administrative burdens this article would imply. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger on-going research or the continuity of the service. Reference was also made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK). ES, FR and IE were broadly supportive of this right. SK thought that the article was unenforceable and DE referred to the difficulty/impossibility to apply this right in 'multi-data subject' cases where a single 'copy' would contain data from several data subjects, who might not necessarily agree or even be known or could not be contacted.

160 DE, IT and SI scrutiny reservation; there is no definition of an 'automated processing system', which could cover almost anything.

161 COM scrutiny reservation.

[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).][162]

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 .][163].

162 FR, HU, SE and UK reservation: this would better set out in the Regulation itself.

163 Text proposed by the Statistics Working Party in 10428/12. Supported by BE, FR, NL and UK. At a later stage, the Commission will look into the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83.

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19
Right to object[164]

1. The data subject shall have the right to object, on reasoned[165] 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)[166]**;** 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[167].

164 DE, ES, EE, AT, SI, SK and UK scrutiny reservation.

165 COM reservation.

166 The reference to point (e) of Article 6(1) was deleted in view of the objections by BE, CZ, DE, DK, FR and HU. COM reservation on deletion. UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. ES and LU queried why Article 6(1) (c) was not listed here.

167 SE scrutiny reservation: SE and NL queried the need to put the burden of proof on the controller regarding the existence of compelling legitimate grounds. DE and FI queried the need for new criteria, other than those from the 1995 Directive. COM stressed that the link with the 'particular situation' was made in order to avoid whimsical objections. CZ also stated that this risked making processing of data an exceptional situation due to the heavy burden of proof. NL and SE queried whether the right would also allow objecting to any processing by third parties.

1a. (…) Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)[168] process the personal data concerned except for the establishment, exercise or defence of legal claims[169].

2. Where personal data are processed for direct marketing[170] purposes, the data subject shall have the right to object **(…)**[171] 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[172].

---

168 ES proposed to reformulate the last part of this paragraph as follows: 'shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise shall no longer use or otherwise process the personal data concerned'.

169 UK proposed adding ' for demonstrating compliance with the obligations imposed under this instrument'. This might also cover the concern raised by DE that a controller should still be able to process data for the execution of a contract if the data were obtained further to a contractual legal basis. CZ, DK, EE, IT, SE and UK have likewise emphasised the need for allowing to demonstrate compliance. CZ and SK also referred to the possibility of further processing on other grounds.

170 FR and UK under lined the need to have clarity regarding the exact content of this concept, possibly through a definition of direct marketing. DE asked which cases were covered exactly.

171 The reference to 'free of charge' was deleted as this already follows from Article 12(4).

172 At the request of several delegations (FR, LT, PT), COM confirmed that this paragraph was not meant to create an opt-in system and that the E-Privacy Directive would remain unaffected. DE feels there is a need to clarify the relationship between Article 19(2) on the one hand and Article 6(1)(f) and Article 6(4) on the other. It can be concluded from the right to object that direct marketing without consent is possible on the basis of a weighing of interests. On the other hand, Article 6(1)(f) no longer refers to the interests of third parties and Article 6(4) also no longer refers to Article 6(1)(f) in regard to data processing which changes the original purpose. DE is therefore of the opinion that this also needs to be clarified in view of online advertising and Directive 2002/58/EC and Article 89 of the Proposal for a Regulation.

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[173]].

[173] Text proposed by the Statistics Working Party in 10428/12. Supported by FR, and DK PL was opposed to this exception. At a later stage, the possibility of consolidating the various paragraphs on statistics into a revised version of Article 83 will need to be looked into.

Article 20

Profiling[174]

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[175] 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[176;] or

---

174 DE, ES, FR, AT, PL, SE and UK scrutiny reservation. COM reservation: COM is of the opinion that that the level of data protection in the current draft of this article is below that of Directive 95/46. DE thinks this provision must take account of two aspects, namely, whether and under what conditions a profile (= the linking of data which permits statements to be made about a data subject's personality) may be created and further processed, and, secondly, under what conditions a purely automated measure based on that profile is permissible if the measure is to the particular disadvantage of the data subject. It appears expedient to include two different rules in this regard. According to DE Article 20 only covers the second aspect and DE would like to see a rule included on profiling in regard to procedures for calculating the probability of specific behaviour (cf. Article 28b of the German Federal Data Protection Act, which requires that a scientifically recognized mathematical/statistical procedure be used which is demonstrably essential as regards the probability of the specific behaviour).

175 DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there are also cases of automated data processing which actually were aimed at increasing the level of data protection (e.g. in case of children that are automatically excluded from certain advertising).

176 NL had proposed to use the wording 'and arrangements allowing him to put his point of view, inspired by Article 15 of Directive 95/46. BE suggested adding this for each case referred in paragraph 2.

(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 [177] are in place.

4. (…)

5. (…)

[177] BE, FR, IT, PL, PT, AT, SE and UK reservation FR and AT reservation on the compatibility with the E-Privacy Directive. BE would prefer to reinstate the term 'solely based', but FR and DE had previously pointed out that 'not … solely' could empty this prohibition of its meaning by allowing sensitive data to be profiled together with other non-sensitive personal data. DE would prefer to insert a reference to a the use of pseudonymous data.

SECTION 5
RESTRICTIONS

Article 21

Restrictions[178]

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[179] and Articles 12 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard[180]:

178 SI and UK scrutiny reservation. SE and UK wondered why paragraph 2 of Article 13 of the 1995 Data Protection Directive had not been copied here. IT and NL also referred to the importance of having the possibility to provide derogations for statistical purposes. DE, supported by DK, HU, RO, PT and SI, stated that para. 1 should not only permit restrictions of the rights of data subjects but also their extension. For example, Article 20(2)(b) requires that Member States lay down 'suitable measures to safeguard the data subject's legitimate interests', which, when they take on the form of extended rights of access to information as provided for under German law in the case of profiling to asses creditworthiness (credit scoring), go beyond the Proposal for a Regulation. With an eye to Article 6(3), the Member States also need flexibility especially in the public sector or in the health sector when it comes to laying down and framing specific rules (esp. in regard to earmarking, the nature of the data and the recipient) and enacting stricter rules. DE and EE thought the derogations should distinguish between the private and the public sector.

179 BE, DE, HU, FI, FR, LU, AT and PL thought that the reference to Article 5 should be deleted, as the principles of Article 5 should never be derogated from. IE and UK opposed this; with IE citing the example of 'unfair' data collection by insurance companies which might be necessary to rebut false damage claims. UK asked for clarification as to why Articles 6-10 are not covered by the exemption.

180 PL deemed such list not appropriate in the context of a Regulation. IT remarked that this demonstrated the impossibility of full harmonisation. GR and LU thought that it needed to be ensured that the exceptions would be interpreted and applied in a restrictive manner.

(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[181], in particular an important[182] economic or financial interest of the Union or of a Member State, including[183], 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.

---

181 DE, IT, LT scrutiny reservation as to the broad character of this exemption. SE thought it should be moved to a separate subparagraph.

182 DK and UK scrutiny reservation on the adjective 'important'.

183 BE and FR suggested adding ' public health' and 'social security'. The Commission's argued that 'public health' was already covered by point (f).

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[184]

SECTION 1
GENERAL OBLIGATIONS

Article 22

Obligations of the controller[185]

1. Taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects[186], the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[187].

---

184 DK, PT, SI and UK scrutiny reservation on the entire chapter. BE stated that it was of the opinion that the proposed rules, while doing away with the general notification obligation on controllers, did not reduce the overall administrative burden/compliance costs for controllers. The Commission disagreed with this. DE, DK, NL, PT and UK were not convinced by the figures provided by COM according to which the reduction of administrative burdens outbalanced any additional burdens flowing from the proposed Regulation. FR referred to the impact this article should have on members of the professions (*professions libéraux*) who collect sensitive data as part of their work (e.g. health professionals)

185 DE scrutiny reservation. UK thought this Article could be deleted as it overlaps with existing obligations. UK thought it focuses too much on procedures rather than on outcomes. DE, LT and PT deplored that Article 22 does not contain an exception for SMEs. BE remarked that anyone who puts a photo on social media might be considered as a controller. SK proposed introducing a new concept of 'entitled person' in Article 4, together with obligations for the controller and processor to instruct their 'entitled persons' who come into contact with personal data about rights and obligations under this regulation as well as laying down responsibility for their infringement.

186 Several delegations stressed that the risk concept should be further detailed: DE, ES, HU, NL, PT, FI and RO. DE, ES and SE pointed out a description or definition of low risk was missing.

187 BE and UK referred to the danger in maintaining such a vaguely worded obligation, applicable to all controllers, non-compliance of which is liable to sanctions.

2. (…)[188]

2a. Where proportionate in relation to the processing activities[189], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller[190].

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 (….)[191].

3. (…)

4. (…)

188 PL asked for the reinstatement of this paragraph.

189 HU and PL thought this wording allowed too much leeway to controllers. AT thought that in particular for the respects to time limits and the reference to the proportionality was problematic.

190 UK thought this was too complicated. ES thought the concept of 'appropriate data protection policies' was too vague.

191 Reference to auditors deleted in view of the remarks made by CZ, ES and IT.

Article 23

Data protection by design and by default[192]

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.[193]

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are not excessive[194] 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[195].

---

192 DE scrutiny reservation; UK reservation: UK thought this should not be set out in the Regulation. FR scrutiny reservation: FR and LT sought clarification on the scope of the data protection by design and by default and on why the processor was not included. DE and MT thought that more emphasis should be put on pseudonymising and anonymising data. DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. It also thought data protection by design and by default should be more used in response to risky data processing operations. ES thought that the term 'non-excessive data processing' was preferable to 'data protection by design'. FR also queried the exact meaning of the terms used in the title.

193 NL stated this paragraph added little in terms of legal obligations compared to other articles in the draft regulation. It might be moved to a recital.

194 ES proposed to replace 'necessary' by 'not excessive in quantity'.

195 DE, IT and SE reservation; DE and UK queried the exact meaning of the last sentence for social media. SE thought this would be better moved to the recitals. BE and FR asked what this added to the principle of data minimisation contained in Article 5. AT thought the second sentence should be retained.

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 [196]

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[197] 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.

---

196 EE scrutiny reservation. SI and UK reservation: UK thought this provision should be deleted. UK and ES thought this article does not take sufficiently account of cloud computing. CZ, DE and NL expressed grave doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings. CZ and DE thought this article should contain a safeguard against outsourcing of responsibility. FR thought the allocation of liability between the controller and the processor is very vague. DE and LT emphasised that it would be in the interest of the data subject to have clear rules and thought the article should therefore be clarified. Other delegations (DK, EE, SE, SI and UK) warned against potential legal conflicts on the allocation of the liability. SE thought that the allocating respective liability between public authorities should be done by legislation. SI scrutiny reservation.

197 BE proposed adding: 'The arrangement shall duly reflect the joint controllers' respective effective roles vis-à-vis data subjects. The arrangement shall designate the supervisory authority in accordance with Article 51. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.' ES suggested adding ' For this agreement to be valid in relation to data subjects, it must be documented and must have been brought to their attention beforehand; otherwise, the aforementioned rights may be exercised in full before any of the controllers, and it shall be incumbent on them to ensure precise compliance with the legally established benefits.' SK also pleaded in favour of informing data subjects of any arrangements between several controllers.

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[198] 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[199]

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union[200].

2. This obligation shall not apply to:

198 DE, FR and LT emphasised that it would be in the interest of the data subject to have clear rules which allow it to address its requests to all controllers concerned. Potential language problems in case of controllers established in different Member States were also highlighted. ES indicated that such arrangements can never be to the detriment of the data subject's rights and its proposal for paragraph 2 seeks to take account of the concerns.

199 DE, GR and UK scrutiny reservation. Several delegations (DE, NL, SE) expressed doubts as to whether the tool of obliging controllers not established in the EU to appoint representatives was the right one to ensure the application of EU data protection law to the offering of services and goods in the EU, in view, inter alia, of the low success of this tool under the 1995 data protection directive. CZ and UK also questioned the enforceability of this provision and thought it should be considered alongside Article 3(2). BE, DE FR, IT, PL and UK argued that, if such obligation were to be imposed, the Regulation, Article 79(6)(f) of which provides a mandatory fine for failure to appoint a representative, should clearly allocate duties and tasks to the representative. Reference was also made to the lack of clarity regarding possible sanctions in case of non-designation of a representative. FR also thought the representative's contact details should mandatorily be communicated to the DPA and referred specifically to the potentially problematic case of non-EU air carriers which, often in cooperation with EU carriers, offered flights to EU residents and might not have a representative in the Union.

200 SI reservation.

(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[201]; 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[202]; or

(c) a public authority or body[203].

(d) (…)[204]

201 BE, DE, IT, NL, PL and SK reservation: they thought this indent should be deleted. At the request of several delegations, COM confirmed that this indent also covered the Safe Harbour Agreement. It also pointed out that under Article 41(2)(1) of its proposal having effective and enforceable rights was precisely one of the determining elements to be taken into account in the case of an adequacy decision.

202 BE, DE, ES, FR, FI, GR, IT, LT,LV, PL, PT and SK remarked that the SME-criterion in itself, while being relevant, could not be sufficient to determine the applicability of the obligation to appoint a representative. The risk inherent in data processing operations should be more important and this text proposal seeks to incorporate this element. DE remarked that the proposed criterion itself would exclude 99.8 % of all enterprises in third countries from the scope of this obligation. FR thought that the risk-criterion should be described in a uniform manner throughout the Regulation

203 SI thought this should be drafted more broadly so as to encompass any body which exercised sovereign governmental powers. LT scrutiny reservation.

204 DE and SK thought that this scenario was not covered by Article 3(2). There appears to be no more need for this subparagraph now in view of the revised recital 23

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[205].

3a. The representative shall be mandated by[206] 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.

205 DE pointed out that paragraph 3 leaves it entirely up to businesses offering EU-wide internet services where they appoint a representative within the EU; it thought that this should be done in accordance with the rule on supervisory jurisdiction in the cases referred to in Article 3(2). At any rate, the supervisory authority in that Member State in which the representative is appointed should have jurisdiction.

206 BE proposed to state 'is liable'.

Article 26

Processor[207]

1. (…)[208] The controller shall <u>use only</u> processor<u>s</u> providing sufficient guarantees[209] to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…)[210].[211]

<u>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.</u>

---

207 CZ reservation: this article should be deleted. Several delegations (DE, EE, FR IT, LU, NL, SI, SK and UK) pointed to the difficulties in distinguishing the roles of controllers and processors, in particular in the context of cloud computing, where the controller often can not exercise (full) control over the way in which the processor handles the data and thought the proposed provision did not reflect the realities of cloud computing. DE thought the provision needed to be re-examined to see to what extent it is applicable to and meaningful for existing and emerging procedures and services in the health sector, in particular the processing of pseudonymised data or data rendered unintelligible and the administration of medical file systems under the patient's control ('Google health', 'health vault').

208 DE proposed starting the sentence by stating that the controller shall be responsible for ensuring compliance with data protection rules.

209 DK and FR thought the 'sufficient guarantees' should be detailed.

210 The latter part of the article was deleted as it added nothing substantial: IE, NL and SE. DE thought it could be put in a separate sentence.

211 Some delegations thought it should be explicitly stated that the rights of the data subject and the right to compensation for damages must be asserted against the controller

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[212] 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 (…)[213], 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 (…)[214];

(e) as far as (…) possible, taking into account the nature of the processing[215], assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;

---

212 FR wanted to know what was meant by an 'other legal act'.

213 DE wondered whether this requirement was feasible in the context of social media.

214 UK thought this overlapped with other parts of the Regulation (Article 26,(2)(a) and 30). BE thought the requirement should be deleted and DE thought it should at least have been limited to establishment of contractual relationships. AT and SK scrutiny reservation: SK thought there were many questions surrounding the relation with this 'secondary' processor.

215 FR thought this was unclear and should possibly replaced by a reference to risk . IT thought different types of risk could be referred to here.

(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[216] 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[217] 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. (…)[218]

[216] Drafting amended in order to accommodate. FR, ES and NL request that there should be an obligation to return the data.

[217] DE referred to 'the principal's rights of supervision and the contractor's corresponding rights of tolerance and involvement', for instance rights of entry, certified auditor's obligations to report periodically.

[218] COM reservation on deletion.

Article 27

Processing under the authority of the controller and processor

(…) [219]

Article 28

Records[220] of categories of personal data processing activities [221]

1. Each controller (…)[222] and, if any, the controller's representative, shall maintain a record of all categories of personal data processing activities under its responsibility[223]. [224]This record shall contain (…) the following information:

---

219 ES, FR, SI and UK stated that it is difficulty to see what is the added value of this Article as compared to Article 26, §2(b). As for employees of the controller, the latter will always be liable for any data protection violations carried out by the former. All confidentiality duties have now been moved to Article 30.

220 Further to UK proposal the term 'document' has been replaced by the more technologically neutral term 'record'. PL and SK suggested to specify that the documents/records could be kept 'in paper or electronically', but the Presidency prefers to keep the wording technologically neutral.

221 AT and SI scrutiny reservation. UK stated that it thought that the administrative burden caused by this Article nullified the benefits if the proposed abolition of the notification obligation. DE, LU, NL and SE shared these concerns.

222 Several delegations (BE, DE) thought the processor should not have cumulative obligations with the controller. ES and UK pointed out that the impact of cloud computing needed further reflection.

223 FR thought it should be specified for how long the documentation needed to be kept.

224 ES proposed to insert a sentence along the following lines: 'Controllers that do not have a data protection officer or sufficient certificate in force, shall have the legally established documentation form with regard to all processing operations carried out under their responsibility'. NL thought the keeping of documentation shoulkd be made conditional upon a prior risk assesment: 'Where a data protection impact assessment as provided for in Article 33 indicates the processing operation presents a high degree of risk, referred to in Article 33'. RO is also in favour of a less prescriptive list.

(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)[225];

(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 (…)[226];

(g) where possible, the envisaged time limits for erasure of the different categories of data.

(h) (…)

2a. Each processor[227] shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:

225 UK suggested deleting it, as it overlaps with Article 6(1)(f).
226 UK reservation.
227 UK thinks this article should not apply to processor(s at all, as all their processing activities are carried out under the responsibility of the controller.

(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[228].

4. The obligations referred to in paragraphs 1 and 2a shall not apply to:

(a) (…)[229]

[228] SI wondered why the data subject was not mentioned here. COM stated this information of the data subject is covered by the general principles. FI proposed to insert an exception in case the controller is subject to a professional secrecy duty, but this is already covered by Article 84 of the regulation.

[229] COM reservation on deletion.

(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[230]; or

(c) categories of processing activities which[231] 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

(…)[232]

230 Many delegations criticised the appropriateness of this criterion: AT, BE, DE, DK, ES, FR, GR, IT, LT, LU, NL, MT, PT, and SE. At the suggestion of BE, the criterion was narrowed in the same way as in Article 25(2)(b).

231 Proposal inspired by Article 18(2) of the Data Protection Directive, in order to take account of delegations that thought that the proposed exceptions were not well-founded and that risk-based exceptions would be preferable. FR thinks that the risk-based approach cannot lead to exemption of certain types of processing operations

232 PT and ES scrutiny reservation on deletion.

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[233] 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. (…)

[233] Several delegations thought that the controller should have the main responsibility (NO, NL, RO, UK).

Article 31

Notification of a personal data breach to the supervisory authority[234]

1. In the case of a personal data breach <u>which is likely to severely affect the rights and freedoms of data subjects</u>[235], the controller shall without undue delay and, where feasible, not later than <u>72</u> hours after having become aware of it, notify the personal data breach to the supervisory authority <u>competent in accordance with Article 51</u>. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within <u>72</u> hours.

1a. <u>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)</u>[236]<u>.</u>

2. (…) The processor shall alert and inform the controller <u>without undue delay after becoming aware</u> of a personal data breach[237] [238].

234 AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

235 BE suggested adding: 'or creates a risk for the data subjects'.

236 BE thought that also point (a) of Article 32(3) should be added here.

237 The Commission highlighted the importance of this obligation, in particular in the context of cloud computing. UK thought this should be moved to Article 26.

238 DE remarked that in view of the Commission proposal of 7 February 2013 for a Directive concerning measures to ensure a high level of network and information security across the Union (COM(2013) 48 final), it should be checked whether in certain cases the authority competent for network and information security should also be notified.

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[239].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).[240]]

239 AT, LU and FR queried what was the retention period for this documentation. IT proposed to insert a reference to the estimated severity of the remedial action taken.

240 BE, DE, IT, LT, RO and UK pleaded for the deletion of paragraph 6.

Article 32

Communication of a personal data breach to the data subject[241]

1. When the personal data breach is likely to <u>severely</u> affect the <u>rights and freedoms</u> of the data subject[242], the controller shall (…)[243] communicate[244] 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[245] the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (<u>e</u>) and (f) of Article 31(3).

3. The communication (…) to the data subject <u>referred to in paragraph 1</u> shall not be required if**:**

241 AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded. NL thought there should be an exception for statistical data processing. FR thought that the possible application to public/private archives required further scrutiny.

242 BE and SK scrutiny reservation. BE suggested adding: 'or creates a risk for the data subjects'.

243 The Presidency agrees with AT, PT and SE that there is no valid reason why the data subject should always be informed after the DPA. Therefore this part has been deleted. DE however proposed to start this paragraph by stating: 'As soon as appropriate measures have been taken to render the data secure or where such measures were not taken without undue delay and there is no longer a risk for the criminal prosecution'

244 PL suggested specifying this could be done either in paper or electronic form.

245 DE proposed adding "in generally comprehensible terms", but this is already covered by Article 12.

a. the controller (…)[246] has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, in particular those that[247] render the data unintelligible to any person who is not authorised to access it, such as encryption or the use of pseudonymous data[248] [249]; 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. (…)

246 NL and FR criticised the subjective criterion of satisfying to the satisfaction of the DPA. More generally, NL opined that there was danger of the data protection authority would obtain company secrets from the data controller which the DPA might be obliged to disclose under access to document legislation.

247 BE proposed 'have the purpose'.

248 AT, FR, IT and PT reservation on reference to pseudonymised data. The Presidency has proposed a new recital 68a to accompany this text.

249 MT and UK thought this exception should also be inserted to Article 31. The Presidency considers that there might be cases where it still might be useful to inform the DPA.

[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).[250]]

[250] BE, CZ, DK, DE, ES, PL and UK pleaded for the deletion of paragraph 6.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment [251]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific[252] risks for the rights and freedoms of data subjects[253], the controller **(…)**[254] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[255].

2. The following processing operations (…) present specific risks referred to in paragraph 1:

---

251 ES, HU and UK scrutiny reservation; FR thought that the possible application to public/private archives required further scrutiny.

252 ES thought that such assessment should not be required in all cases and wanted to restrict the scope of the Article. ES, FR, LU, PT, RO, SK, SI and UK warned against the considerable administrative burdens flowing from the proposed obligation.

253 BE scrutiny reservation.

254 Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deletion.

255 ES had proposed exempting certified processing operations. BE, CZ, EE and had proposed exempting a controller who had appointed a DPO.

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[256] are based that produce legal effects concerning data subjects or severely affect data subjects[257];

(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[258];

(c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (…)[259];

256 BE proposed to replace this by wording similar to that used for profiling in Article 20: 'decision which produces adverse legal effects concerning this natural person or significant adverse effects concerning this natural person'. DE and NL also thought the drafting could be improved.

257 FR thought profiling measures might need to be covered by this Article, but the Presidency thinks this type of processing is largely covered by paragraph 2(a).

258 DE proposed referring to 'particularly sensitive personal information, in particular special categories of personal data under Article 9(1), data on children, genetic data or biometric data'. FR and IT are also supportive of the inclusion on sensitive data.

259 BE, FR, SK and IT asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale'. DE proposed the following text: 'processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where legitimate expectations are not met, for example owing to the context of the processing operation'.

(d) personal data in large scale processing systems containing genetic data or biometric data[260];

(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[261].

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. [262]

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. [263]

260 COM reservation on deletion of reference to children. DE proposed 'processing operations which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons'.

261 BE and DE reservation: in favour of deleting this subparagraph. NL and PL thought a role could be given to the EDPB in order to determine high-risk operations.

262 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

263 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

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[264], safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[265], taking into account the rights and legitimate interests of data subjects and other persons concerned[266].

4. (…)[267]

5. Where a controller is a public authority or body[268] 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[269].

6. (…)

7. (…)

264 DE suggests adding ' also in view of Article 30'.

265 NL proposes to specify this reference and refer to Articles 30, 31, 32 and 35.

266 DE and FR scrutiny reservation. DE referred to Article 23 (b) of the 2008 Data Protection Framework Decision, which requires prior consultation of the DPA where 'the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.'

267 The Presidency agrees with those delegations (BE, FR) that indicated that this was a completely impractical obligation. NL and COM were in favour of maintaining it.

268 BE proposed replacing the criterion of a controller being a public body by 'data are processed for the public interest'.

269 IT scrutiny reservation. DK, IT and COM think the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

Article 34

Prior (…) consultation[270]

1. (…)

2. The controller **(…)**[271] 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[272] [273].

(…)

[270] ES, HU and UK scrutiny reservation; DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. The Presidency has revised the wording of recital 74 with a view to clarifying the scope of the obligation.

[271] Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deleting processor.

[272] FR and SE scrutiny reservation on the concept of a high degree of specific risks.It was pointed out that such assesments might be time-consuming. IT thought there should be scope for consulting the DPA in other cases as well.

[273] DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

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 (…)[274]. 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[275].

4. (…)

5. (…)[276]

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 (…).[277].

274 Drafting amended in order to take account of the concern expressed by several delegations that a sanctioning power for DPAs would be difficult to reconcile with (1) the duty on controllers to make prior consultation under the previous paragraph (DE, DK, NL, SE, SI) and (2) the freedom of expression (NL, PL, SI).

275 ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing. The Presidency thinks that any discussion regarding differentiating the DPA powers should take place under Article 53.

276 IT reservation on the deletion of paragraphs 4 and 5.

277 DE thought this paragraph should be deleted.

7. Member States shall consult the supervisory authority during the preparation[278] of proposals for legislative or regulatory measures which provide for the processing of personal data and which may severely[279] 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[280].

8. (…)

9. (…)

[278] CZ wanted clarification that this obligation does not apply to private member's bills.

[279] COM reservation, in particular regarding regulatory measures: this threshold is not present in the 1995 Directive.

[280] DK, NL, PL, SE scrutiny reservation.

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,[281] designate a data protection officer (…)[282].

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[283] (…).

6. (…)

---

281 Made optional further to decision by the Council. DE and AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself. COM reservation on optional nature and deletion of points a) to c). UK thinks paragraphs 5 to 8 could be deleted.

282 PL suggested adding 'The controller or the processor may appoint one or more deputy data protection officers. Deputy data protection officer must fulfil conditions stipulated in art. 35 point 5 of this Regulation"

283 PL suggested adding a reference to the absence of a criminal record as a condition.

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[284]

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.

[284] UK thought articles 36 and 37 could be deleted in a pure risk-based approach.

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[285] 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[286].

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;

---

285 DE, EE, ES, LV and NL pointed out that the requirement of independence was not the same for DPOs as for DPAs.

286 Moved from Article 35 (6). DE was opposed to this as these requirements were irrelevant to the functional independence of the DPO. FR demanded further clarifications. UK also thought this was too prescriptive. Presidency endeavoured to redraft this paragraph in order to make it less prescriptive. AT thought the redraft did not sufficiently take account of the situation of external DPOs.

(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[287].

2. (….)

[287] FR suggested adding an obligation to draft an annual report on his activities, but the Presidency wonders whether this is not too heavy an obligation.

SECTION 5

CODES OF CONDUCT AND CERTIFICATION[288]

Article 38

Codes of conduct [289][290]

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[291] 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;

288 COM scrutiny reservation on Section 5.

289 AT, DK, FI, SK and PL scrutiny reservation. DE, FR and SI stated that this article should not apply to the public sector.

290 Several delegations thought more incentives should be made to apply to the use of codes of conduct: BE, DE, DK, LV, SE, SI, UK. Several delegations thought that hortatory language was being used in §1 (SI, PT), §1c (NL, SI, FR)

291 LU pleaded in favour of extending this to multinational companies established in various Member states.

(bb) the use of pseudonymous data[292];

(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[293].

[292] FR scrutiny reservation.

[293] NL queried whether this also covered the transfer to processors in 3rd countries.

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[294] 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[295] (…).

---

294 Further to CY, FR, IT, LU, LV and PT suggestion.

295 DE, IE, ES, PT also remarked that the DPAs should be involved; to that end paragraph 2a has been inserted. EE, ES and UK thought that the Commission need not be involved.

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[296]. 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[297].

Article 38a

Monitoring (…) of codes of conduct[298]

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[299] 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;

296 CZ, EE and FR queried what was the legal status of such approved codes of conduct and in particular their binding nature.

297 BG suggests deleting paragraph 4; ES suggests deleting paragraphs 4 and 5.

298 AT, DE , DK, NL, LU, FI, ,IT , PT and UK scrutiny reservation.

299 CZ, DK, EE, LV, PT and UK are opposed to giving this role to such separate bodies. Concerns were raised, *inter alia*, on the administrative burden involved in the setting up of such bodies. The Presidency stresses that codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

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 **(…)** demonstrate**s** 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[300].

6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Article 39

Certification[301]

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.

(…)

300 BE proposed adding: 'An infringement of a code of conduct shall not in itself constitute an infringement of this Regulation, unless the Commission has, pursuant to paragraph 4 of Article 38, decided the code has general validity within the European Union.' The Presidency thinks that this proposal should be revisited in the wider context of the discussions on sanctions.

301 AT, DK, EE, FR, FI , IT , PT and UK scrutiny reservation. ES, SI and UK thought further incentives should be provided for using certification mechanism. FR thought the terminology used was unclear an that the DPA should be in a position to check compliance with certified data protection policies; the Presidency will try to do this in Article 53.

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[302]

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;

[302] AT, DK, EE, FR, IT and PT scrutiny reservation.

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 (…) demonstrate**s** 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)[303].

[303] DE pleaded in favour of deleting the last two paragraphs. ES thought that this should not be left exclusively to the Commission.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[304]

Article 40

General principle for transfers[305]

(…)[306].

304 FR reservation. In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, CZ, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (EE, FR, PL). FR requested that a grandfather clause be inserted preserving international agreements concluded by Member States.

305 COM scrutiny reservation, in particular regards onward transfers.

306 The Presidency agrees with GR, SE, NL and UK that this article has no added value to the rest of the Chapter V and has therefore deleted it., BE, supported by FI and NL, thought that the requirements regarding onward transfer need not be mentioned here, as these were at any rate subsumed under the adequacy requirement. FR thought the requirement of prior originator consent to onward transfer should be expressed in a different manner. ES was opposed to putting the processor and controller on the same footing.

Article 41

Transfers with an adequacy decision[307]

1. A transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where the Commission[308] has decided that the third country, or a territory or a processing sector[309] within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific[310] authorisation.

2. When assessing the adequacy of the level of protection, the Commission[311][312] shall, in particular, take account of[313] the following elements:

   (a) the rule of law, respect for human rights[314] and fundamental freedoms, relevant legislation (…), data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, as well as the existence of effective

---

307 AT, LU and FR expressed their support for maintaining the adequacy procedure. Some delegations raised concerns on the time taken up by adequacy procedures. LV thought a separate paragraph setting.

308 CZ and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data. UK had considerable doubts on the feasibility of the list in paragraph 2.

309 IT, SK and AT scrutiny reservation.

310 ES proposal.

311 NL thought a preponderant role should be given to the EDPB in assessing these elements. COM indicated that this could be done in the articles dealing with the EDPB competences and that at any rate the Member States were involved in the adequacy procedure.

312 CZ and IT asked for involvement of the EDPB.

313 PL proposal. IT thought the list should not be exhaustive and therefore proposed adding 'in particular'.

314 GR, AT and SK thought a reference to human rights should be inserted.

and enforceable[315] data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred(…)[316],[317];

(b) the existence and effective functioning of one or more independent[318] supervisory authorities[319] in the third country, or to which an international organisation is subject, with responsibility for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation concerned has entered into[320] in relation to the protection of personal data[321] **[322]**,

315 ES proposal.

316 Deleted further to CZ and FI remark that no distinction should be made between EU citizens.

317 COM scrutiny reservation.

318 Further to FDE and BE proposal.

319 CZ and NL queried how strict this independence would need to be assessed.

320 CH and NL remarked that many of these elements need to be formulated less broadly. FR thought the criteria should be more focused on implementation.

321 CZ proposal. COM had clarified that this was mainly the CoE Convention No 108.

322 DE proposed adding ' participation in a suitable international data protection system established in third countries or a territory or a processing sector' and that the list of checks in Article 42(2) should include a new component consisting of the participation of third States or international organisations in international data-protection systems (e.g. APEC and ECOWAS). It also suggested referring to 'ways of ensuring consistent interpretation and application of the data-protection provisions under Articles 55 et seq'.

3. The Commission, after assessing the adequacy [323] of the level of protection, may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure[324] referred to in Article 87(2).[325]

3a *Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[326].

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.

---

323 DE proposal. CZ and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data.

324 BE and LU queried whether Member States would initiate such procedure.

325 DE queried the follow-up to such decisions and warned against the danger that third countries benefiting from an adequacy decision might not continue to offer the same level of data protection. COM indicated there was monitoring of third countries for which an adequacy decision was taken.

326 Moved from paragraph 8. CZ and AT thought an absolute time period should be set.NL, PT and SI thought this paragraph 8 was superfluous or at least unclear. If maintained it should be moved to the end of the Regulation.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer[327] ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3).[328]

6. (…) A decision (…) pursuant to paragraph 5 (…) is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44 (…). At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.[329]

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)[330]

---

327 COM reservation on the deletion of its possibility to adopt negative adequacy decisions.

328 BE, DE, FI, IT, LU and FR asked for the deletion of paragraph 5.

329 BE, DE, FR, FI, IT, LU and CZ asked for the deletion of paragraph 6.

330 Move to paragraph 3a.

Article 42

Transfers by way of appropriate safeguards[331]

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards[332] *in a legally binding instrument* with respect to the protection of personal data (…).

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular[333], by:

   (a) binding corporate rules pursuant to Article 43; or

   (b) standard data protection clauses adopted by the Commission[334] (…) in accordance with the examination procedure referred to in Article 87(2); or

   (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2)[335]; or

331 Several delegations (BE, CH, IT) queried whether this article (in particular paragraphs 2 (a + b) and 5 could also be applied to public authorities UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of this procedures regarding data flows in the context of cloud computing was also questioned.

332 SK scrutiny reservation.

333 COM emphasised the non-exhaustive nature of this list, clarifying that also other types of agreements could be envisaged.

334 FR reservation.

335 DE proposal.

(d) contractual clauses between the controller or processor and the recipient of the data[336] authorised by a supervisory authority pursuant to paragraph 4; or

(e) an approved code of conduct pursuant to Article 38[337]; or

(f) a certification mechanism pursuant to Article 39. [338], **[339]**

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

4. Where a transfer is based on contractual clauses as referred to in point (d)[340] of paragraph 2 (…) [341], the controller or processor[342] shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…).

5. [343]Where, nothwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor, being a public authority or body, shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).

---

336 BE proposed referring to a sub-processor.

337 COM scrutiny reservation.

338 NL proposed adding a reference to 'mutual binding obligations of professional secrecy or existing sectoral legislation which offers special protection to the interests of data subject between the controller or processor and the recipient of the data in the third country, territory or processing sector thereof or international organisation'.

339 COM scrutiny reservation.

340 BE proposed adding a reference point (e). CH thought this paragraph should not be applicable to public authorities.

341 ES suggested inserting a reference to the absence of a DPO or certifications.

342 BE suggested deleting the reference to the processor.

343 BE and GR want to limit the scope of this paragraph to public authorities. IT on the contrary could not see how it could be applied by public authorities.

5a. If the transfer referred to in paragraph 4 (…)[344] is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority*[345]

6. (…)[346].

344 COM scrutiny reservation.

345 UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. It was thought that this was contrary to the principle of accountability. The question as to the fate of existing MOUs and international conventions was also raised. AT, PL, GR, SI and BG voiced concerns regarding the possibility to transfer personal data in the absence of a legally binding instrument. FR scrutiny reservation on the terms 'administrative arrangements' and 'substantially affect the free movement of personal data'. BE also thought this paragraph needed clarification.

346 Subsumed under paragraphs 4 and 5.

Article 43

Transfers by way of binding corporate rules[347]

1. The competent supervisory authority shall *approve*[348] *binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they:

   (a) are legally binding and apply to, and are enforced by, every member concerned[349] of the group of undertakings or group of enterprises engaged in a joint economic activity[350],[351],[352];

   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data[353];

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

---

347 Several delegations supported this innovative legal technique: BE, CZ, DE, FR, FI, IT, LU, NL, PT and PL. NL thought it should be given a wider scope. NL and GR pleaded in favour of covering data flows in the context of cloud computing and ES thought more flexibility should be provided in this way. SI thought it should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied.

348 DE and UK expressed concerns on the lengthiness and cost of such approval procedures. The question was raised which DPAs should be involved in the approval of such BCRs in the consistency mechanism.

349 DE proposal.

350 Further to GR proposed to insert a reference to 'alliances'. BE proposed to refer to sub-processors; ES proposed to insert a reference (in paragraph 1(a) as well as in (2)(f)(h)(i) and (k) to 'business partners'.

351 NL asked whether the BCRs should also be binding upon employees. ES thought subparagraph (a) could be simplified by stating that BCRs all binding to all involved.

352 COM has a scrutiny reservation on ‘group of enterprises engaged in a joint economic activity’ extending the scope beyond one group of undertakings and how this would work in practice.

353 FI proposed referring to BCRs and BE suggested a reference to effective administrative and judicial redress.

2. The binding corporate rules referred to in paragraph 1 shall at least[354] specify the following elements:

(a) the structure and contact details of the group concerned[355] and of each of its members[356];

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

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

(d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing[357], data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data[358] and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

354 FR pleaded in favour of deleting the words 'at least'. IT is opposed to the deletion thereof.
355 BE proposals.
356 BE proposal; BE also proposed a reference to sub-processors.
357 NL proposal.
358 FI proposal.

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

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

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

(hh) the complaint procedures;

(i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules[359];

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

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

[359] NL proposed referring to auditing as an example.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.][360]

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

Article 44

Derogations for specific situations[361]

1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42[362], a transfer or a category of transfers[363] of personal data to a third country or an international organisation may take place only on condition that:

360 CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives.

361 EE, FR and NL reservation. UK thought that in reality these 'derogation' would become the main basis for international data transfers. It also opined that by their nature (many of) these derogations should not be called as such because the data transfers for which the allow are both justified and necessary.

362 BE and LU proposed adding a reference to BCRs.

363 FR and PL scrutiny reservation on the term 'set of transfers'.

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

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

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

(d) the transfer is necessary for *important* reasons of (…) public interest[364]; *this must be a public interest recognised**[365]** in Union law or in the national law of the Member State to which the controller is subject* ; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims[366]; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent**[367]**; or

---

364 DE remarked that the effects of (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties. FR and IT reservation on the (subjective) use of the concept of public interest. It thought that also here it should be clarified that this ground cannot justify massive and structural transfers of data.LU proposed deleting the word 'important'.

365 According to DE the word "exist" should make it clear that it is the public interest of the EU Member State being referred to, and not that of the third state.

366 PL requested clarification on this subparagraph.

367 In the view of the Presidency this also covers public health emergency situations.

[(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case[368];]**[369]** or

(h) the transfer *which* is not large scale or *frequent*[370], is necessary for the purposes of legitimate interests pursued by the controller or the processor[371] and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, *where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data[372];.**[373]**

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

---

368 FI requested clarification of this subparagraph.

369 The Presidency will request the Commission to explain the purpose of this provision.

370 NL proposal. DE and SK also thought the terms 'frequent or massive' are unclear. UK thought this qualification should be deleted.

371 FR requests clarification concerning the concept of "legitimate interest(s)" and would like the balance of Directive 95/46 to be preserved. It scrutiny reservation. AT, PT and PL are opposed to this subparagraph and plead in favour of its deletion.

372 IT suggested deleting the words 'where necessary'.

373 DE proposed adding another exemption in cases where the competent supervisory authority has granted prior authorisation. DE is of the opinion: public entities should be exempted from this provision, because they are already checked by a state authority, which is itself subject to supervision and involved in procedures of mutual administrative and legal assistance.

3. (…)

4. Points (a), (b) and (c) of paragraph 1[374] shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. (…).[375]

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…) [376].

[6a International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked.][377]

7. (…)[378].

374 COM scrutiny reservation on deleting (h).

375 Moved to paragraph (1)(d). DE and NL proposed adding the possibility of Member State law preventing a transfer of data outside the EU.

376 GR reservation: GR suggested deleting this paragraph in view of the administrative burden it entailed for controllers. IT wanted to clarify the notification took place before the transfer.

377 COM enters reservation based on strong legal doubts on the legality of such proposal. COM recalls recital 79 which states that 'This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subject.'

378 Deleted further to reservation by BE, CZ, CY, ES, FR, FI, SE and UK.

Article 45

International co-operation for the protection of personal data[379]

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

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

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) , complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[380];

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

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

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3)[381].

379 PL thought (part of)Article 45 could be inserted into the preamble. UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI.

380 AT and FO thought this subparagraph was unclear and required clarification.

381 NL suggested deleting this paragraph.

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46

Supervisory authority[382]

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Regulation.

1a Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union (…)[383]. For this purpose, the supervisory authorities shall co-operate with each other and the Commission[384].

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which shall represent those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57[385].

382 At the request of IT, COM clarified that this DPA could be the same as the one designated/set up under the future Data Protection Directive. ES asked for clarification that a DPA may be composed of more members, but the presidency thinks this is already sufficiently clear from the current text.

383 UK sought reassurance that the supervisory authority could also be given a wider remit, such as ensuring the freedom of information.

384 UK thought there was no reason to mention this duty of co-operation here.

385 De suggested deleting the bracketed part of the text

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them[386].

Article 47

Independence

1. Each supervisory authority shall act with complete[387] independence in performing the duties[388] and *exercising* the powers entrusted to it (…).

2. The member or members of each supervisory authority shall, in the performance of their duties and exercise of their powers, remain free from external influence, whether direct or indirect.

3. (…)

4. (…)[389]

5. Each Member State shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and exercise of its powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board[390].

386 This paragraph could be moved to the final provisions.
387 EE and SI suggested deleting the word 'completely'.
388 GR scrutiny reservation.
389 COM scrutiny reservation on deletion of paragraphs 3 and 4.
390 This paragraph was criticised for being too prescriptive (FR, SE) and too vague (LV).

6. Each Member State shall ensure that each supervisory authority has its own staff which shall (…) be subject to the direction of the member or members[391] of the supervisory authority.

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

Article 48

General conditions for the members of the supervisory authority

1. Member States shall provide that the member or members[392] of each supervisory authority must be appointed either by the parliament or the government or the head of State of the Member State concerned[393].

2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers (…)[394].

3. (…)

4. (…).

5. (…)[395].

---

391 DE, LV, NO, PT and UK questioned who were to be considered as members of the DPA and argued that the regulation should allow different models. IT thought EU resources could also be considered.

392 DE, LV, NO, PT and UK questioned would were to be considered as members of the DPA and argued that the regulation should allow different models.

393 Several delegations (FR, SE, SI and UK) thought that other modes of appointment should be allowed for. LU thought this should not be governed by the Regulation.

394 As several delegations (DE, ES, SE) thought that also the appointment of persons with prior data protection experience should be allowed for, this requirement has been deleted. CZ indicated that independence should not be a requirement for appointment, but for the functioning of DPA members.

395 The Presidency agrees with those delegations (BE, CZ, FR, LU, NL, NO, PT, SE, SK, UK) that are of the opinion that paragraphs 4 and 5 interfere too much with national law. CZ, NO, SE and the Presidency also see no need for paragraph 3. COM scrutiny reservation on deletion of paragraphs 3 to 5.

Article 49

Rules on the establishment of the supervisory authority [396]

1. Each Member State shall provide by law for:

(a) the establishment (…) of <u>each</u> supervisory authority;

(b) (…);

(c) the rules and procedures for the appointment of the <u>member or</u> members of <u>each</u> supervisory authority (…);

(d) the duration of the term of the <u>member or</u> members of <u>each</u> supervisory authority which shall <u>not</u> be[397] (…) less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure[398];

(e) whether <u>and, if so, for how many terms</u>[399] the <u>member or</u> members of <u>each</u> supervisory authority shall be eligible for reappointment;

396 DE and FR queried which was the leeway given to Member States by this article as compared to the rules flowing from the previous Articles from the Regulation. Several delegations (FR, GR, SE, SI UK) thought that some of these rules, in particular those spelled out in subparagraphs (c) and (d) were too detailed.

397 DE proposed adding a maximum term of eight years.

398 The last part of this point might need to be moved to the final provisions.

399 DE proposal. IT likewise thought a maximum term should be set

(f) the (…) conditions governing the employment of the member or members and staff of each supervisory authority and rules governing the cessation of employment[400];

(g) (…).

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their (…) duties or exercise of their powers, *both during and after their term of office*.[401], [402]

Article 50

Professional secrecy[403]

(…)

400 SE thought that subparagraphs (b), (c) and (f) should be deleted or substantially redrafted as they were too detailed.

401 BE proposed adding an additional paragraph on the need to distinguish investigating and sanctioning powers, but the presidency deem that this is dealt with by the general safeguard clause in Article 53.5. The same goes for the DE proposal for adding language concerning the duty to report an offence under national law and the privilege against self-incrimination.

402 COM scrutiny reservation on adding the provision on professional secrecy to Article 49, which concerns rules on the establishment of supervisory authorities.

403 UK pointed out that also transparency concerns should be taken into account. Many delegations (CZ, DE, FR, FI; GR, IT, SE, SI, UK) raised practical questions as to the scope and the exact implications of this article. All thought that the rules on professional secrecy should be left to national law and hence the Presidency has followed the suggestion by CZ and SI and moved this to Article 49. COM scrutiny reservation on moving this provision to Article 49; should remain a separate provision.

SECTION 2

COMPETENCE[404], DUTIES AND POWERS

Article 51

Competence[405]

1. Each supervisory authority shall be competent to perform the duties and to exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State[406].[407]

404 GR thought it would be better to refer to jurisdiction rather than competence.

405 Some delegations (BG, CY, DE, GR, NL and LU) supported the principle of the main-establishment rule (aka as the one-stop-shop principle), but had many questions of understanding as to its practical implementation. Other delegations (BE, CZ, ES, FR, IT, AT, PT, RO and SI) had a more critical attitude and entered a reservation. One of the main questions was whether the allocation of competence to the DPA of the main establishment was exclusive and whether it also implied a rule of applicable law (DE, ES). A practical question was that of the language regime which would govern the co-operation between the DPAs and the communication with the controllers and the data protection. All delegations seemed to agree that at any rate the establishment of such a rule could not lead to the exercise of investigative powers by the DPA of one authority in the territory of another Member State.

406 At the request of several delegations, COM indicated that the main-establishment rule under this paragraph would not apply to controllers established outside the EU. In the view of the Commission, this constituted an incentive for non-EU controllers to establish themselves in the EU in order to avail themselves of the benefit of the main establishment rule. PL rightly pointed out that there was a need to specify the criterion on the basis of which the competent DPA would be established in such cases and the Presidency has endeavoured to do so by adding a sentence.

407 Some Member States questioned the interaction between paragraphs 1 and 2 and requested more clarity on which was to be the competent Member State: DE, SE. The Presidency has endeavoured to redraft paragraph 1 so as to clarify that this paragraph sets out the principle of the territoriality of supervision, from which the main-establishment rule in paragraph 2 derogates. The new drafting of § 1 also implies that for controllers established outside the EU, the competent DPA will be that of the Member State where the data subjects resides. IT thought the latter rule should also be applied regarding pricessing of personal dat by controllers/processors established within the EU.

2. Where the processing of personal data takes place within several Member States and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for measures intended to produce legal effects by performing the duties pursuant to points (hb) and (i) of Article 52(1) and exercising the powers pursuant to points (a) to (h) of Article 53(1) and Articles 79 and 79a as regards the processing activities of the controller or the processor in all Member States concerned.

2a. The supervisory authority of the main establishment shall cooperate with other supervisory authorities and, in particular, with the supervisory authority to which a complaint has been lodged, pursuant to the provisions of Chapter VII of this Regulation.

2b. Paragraph 2 shall not apply to public authorities and bodies[408].

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[409].

[408] Further to LU proposal.
[409] FR, HU, UK scrutiny reservation.

Article 52

Duties[410]

1. Each supervisory authority shall at least[411]:

(aa) *promote (…) public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention*;

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

(ac) *upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;*.

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

(b) deal with complaints[412] lodged by a data subject, or body, organisation or[413] association representing a data subject in accordance with Article 73, and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period[414], in particular if further investigation or coordination with another supervisory authority is necessary;

410 IT scrutiny reservation.
411 Addition suggested by the Presidency in order to clarify that Member States may allocate other tasks to DPAs.
412 IT scrutiny reservation on the term complaint; UK thought the emphasis should be on complaint-resolution.
413 Alignment with the text of Article 73.
414 IT suggested fixing a 10-weeks period for dealing with the complaint.

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

(d) conduct investigations on the application of this Regulation either on its own initiative or on the basis of a (…) request of another supervisory or other public authority (…);

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

(f) respond to consultation requests by Member State institutions and bodies, including those pursuant to paragraph 7 of Article 34, on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data[415];

(fa) establish and make public a list in relation to the requirement for a data protection impact assessment pursuant to Article 33(2a)[416];

(g) give advice on the processing operations referred to in Article 34(3) and authorise processing referred to in Article 34(7a);

(ga) encourage the drawing up of codes of conduct pursuant to Article 38;

---

415 CZ, ES, MT and LT reservation on this measure, which they considered as an interference with the legislative process. Other delegations (CH, DE, FI, LU, SI) did not have problems with this obligation, which already existed under the data protection Directive 46/95

416 Further to BE proposal.

(gb) promote the establishment of data protection certification mechanisms and of data protection seals and marks;

(gc) carry out a periodic review of certifications issued in accordance with Article 39(4);

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

(ha) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a[417];

(hb) authorise contractual clauses referred to in Article 42(2)(d);

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

(j) contribute to the activities of the European Data Protection Board.

2. (…)[418]

3. (…)[419]

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

5. The performance of the duties of each supervisory authority shall be free of charge for the data subject and for the data protection officer[420].

417 Further to DE proposal.
418 Moved to paragraph 1.
419 Moved to paragraph 1.
420 DE proposal.

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on[421] the request (…) [422]. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[423].

Article 53

***Powers*[424]**

1. Each Member State shall provide by law that[425] its supervisory authority shall have at least[426] the following powers[427]:

421 DE proposal.

422 PL scrutiny reservation. EE pointed out that under its constitution this required an act of parliament. NL also thought this should be left to Member States.

423 DE reservation: this can be left to general rules.

424 Several Member States (DE, FR) stated that it was unacceptable that the supervisory authority would be able to exercise these powers vis-à-vis public authorities.

425 Suggested amendment in order to allay the concern from Member States (FR, NL) that they should be able to specify in their national law, as has been the case under the 1995 Data Protection Directive, the exact scope of, conditions and guarantees for the exercise of these powers.

426 Further to BG suggestion to make this an indicative list. RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules.

427 A distinction must be drawn between powers with regard to public and non-public bodies. Direct powers of instruction in respect of public bodies subject to supervisory and judicial control, which might therefore lead to conflicts, would be problematic for Germany. Moreover, consideration also needs to be given to the delimitation between this proposal and the proposal for a Directive on police and judicial affairs, which accords fewer powers to the supervisory authorities in some respects.

(a) to notify the controller or the processor of an alleged infringement of this Regulation, and, where appropriate, order the controller or the processor to remedy that infringement[428];

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

(ba) to carry out data protection audits;

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

(d) to ensure (…) compliance with the requirement for prior consultations referred to in Article 34(2) and prior authorisations referred to in Article 34(7a) and Article 42(2)(d) and (5);

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

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

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

[428] BE suggested adding the power to oblige the controller to communicate the personal data breach to the data subject.

(f) to order the rectification, restriction or erasure (…) of (…) data (…)[429] and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17 and 17b;

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

(h) to order the suspension of data flows to a recipient in a third country or to an international organisation;

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

(j) (…)[430].

2. Each supervisory authority shall have (…) power to obtain, from the controller or the processor:

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

(b) access to any of its premises, including to any data processing equipment and means (…)[431].

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

---

429 Deleted further to DE suggestion as the breach of the Regulation is obvious here.

430 Deleted in view of the constitutional and other problems raised by some Member States (NL, IT, PT) and the fact that there is already an information under Article 54. ES suggested inserting a reference to the carrying out of audit plans or audit plans.

431 The requirement of reasonable grounds has been deleted here as the procedural requirements will be set out under national law to which the new paragraph 5 refers.

3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and to commence or engage in legal proceedings[432], in order to enforce the provisions of this Regulation.

4. Each supervisory authority shall have the power to impose an administrative fine pursuant to Articles 79 and 79a in addition to, or instead of, measures referred to in points (e) to (h) of paragraph 1, depending on the circumstances of each individual case,.[433].

5. The exercise by a supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process[434].

---

432 CZ, DE and FR reservation on proposed DPA power to engage in legal proceedings.

433 BE scrutiny reservation. DE reservation: deletion.

434 New paragraph, partially inspired by the last sentence of paragraph 2. The additional language is proposed by the Presidency in order to clarify that these powers will be exercised under the national law of the Member States, which needs to provide for the necessary guarantees for the rights of the defence. The reference to national law will allow Member States to apply their procedural rules (cf. remarks by BE, DE, ES). This should also allow to take into account any concerns regarding self-incrimination.

Article 54

Activity report

Each supervisory authority shall draw up an annual report[435] on its activities. The report shall be transmitted to the government[436] and the national parliament and shall be made available to the public, the Commission and the European Data Protection Board.

435 This article does not detract from the possibility for Member States to provide under national law that other, extraordinary reports may also be conveyed to the parliament and the government. However, the Presidency agrees with SI that there no need to oblige Member States to do so, certainly as there is a risk of an 'overkill' of reports.

436 SE proposal; ES suggested adding 'other authorities designated under national law'.

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 54a

Cooperation in case of complaints

1. Where a complaint has been lodged with a supervisory authority other than the one which is competent pursuant to Article 51, the competent supervisory authority shall, on receiving the complaint, take appropriate measures in consultation with the supervisory authority to which the complaint has been lodged.

2. When exercising the powers referred to in paragraph 2 of Article 51, the competent supervisory authority shall take utmost account of the views of the supervisory authority to which the complaint has been lodged.

Article 55

Mutual assistance[437]

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. This shall apply in particular where the supervisory authority to which the complaint has been lodged is not the authority of the main establishment of the controller or processor. Mutual assistance shall also cover the provision of information on the conduct of investigations where data subjects in several Member States are likely to be affected by processing operations by the controller or processor.

437 SI and SE scrutiny reservation. Several delegations indicated further clarity was required on the concept of mutual assistance: DE, NL, FR, ES, NL , PL and UK pleaded for more flexibility. COM stated this was a specification of the rules already contained in CoE Convention No. 108. EE pleaded for much more detailed rules on mutual assistance, as is already the case in civil and criminal law.

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month[438] after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation or enforcement measures to bring about the suspension or prohibition of processing operations which infringe this Regulation.

3. The request for assistance shall contain all the necessary information[439], including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. [440]A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent for the subject-matter of the request[441]; or

(b) compliance with the request would be incompatible with the provisions of this Regulation or with Union or Member State law to which the supervisory authority receiving the request is subject.

438 SE remarked that this timeline might be unrealistic in some cases. COM indicated that it was only a deadline for replying, but that §5 allowed longer periods for executing the assistance requested ES on the other hand suggested reducing it to 15 days.

439 EE scrutiny reservation.

440 SE indicated further scrutiny was required as to whether other grounds of refusal were required.

441 Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request[442].

6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means (…), using a standardised format.

7. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorites rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5[443] within one month of receiving the request[444] of another suervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board and the Commission in accordance with the consistency mechanism referred to in Article 57[445].

442 Further to IT remark
443 SE suggestion.
444 Further to DE and GR suggestion.
445 EE, FR, RO and UK reservation. FR asked whether this referred to the urgency procedure of Article 61.

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board and to the Commission in accordance with the consistency mechanism referred to in Article 57.

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)[446].

Article 56

***Joint operations of supervisory authorities*[447]**

1. (…) The supervisory authorities may[448], where appropriate, conduct *joint operations,* including joint investigatons and joint enforcement measures (…) in which (…) members or staff from other Member States' supervisory authorities are involved.

446 DE, IT and EE reservation. EE questioned whether implementing acts where necessary for this purpose .

447 EE and PT scrutiny reservation. Several delegations (DE, LV, NL, SE) supported the idea of joint operations, but thought more details needed to clarified. DE and EE referred to a criminal law model of a joint investigation team. Other Member States (LU, PL) indicated they were not convinced of the added value of joint investigations.

448 LU proposal.

2. In cases where a significant number of[449] data subjects in several Member States are likely to be adversely[450] affected by processing operations[451], a supervisory authority of each of those Member States shall have the right to participate in the (…) joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the (…) joint operations concerned and respond to the request of a supervisory authority to participate (…) without delay.

3. A supervisory authority may, (…) in compliance with its own Member State law, and with the seconding supervisory authority's authorisation, confer (…) powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the seconding supervisory authority's law. Such investigative powers may be exercised only under the guidance and (…) in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…)[452].[453]

4. (…)

449 LU proposal. COM reservation.
450 LU and SI suggestion.
451 At the request of several delegations, COM indicated that this phrase was the criterion which could trigger the establishment of a joint operation.
452 SI and GR suggestion.
453 DE and COM scrutiny reservation.

5. Where a joint operation is intended and a supervisory authority does not comply within one month with the obligation laid down in the second sentence of paragraph 2, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5, which shall not exceed three months. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board and to the Commission (…) in accordance with the consistency mechanism referred to in Article 57.

SECTION 2

CONSISTENCY[454]

Article 57

Consistency mechanism

1. For the purpose set out in Article 46(1a), the supervisory authorities shall co-operate with each other through the consistency mechanism as set out in this section[455].

2. Before the competent supervisory authority adopts a measure referred to in paragraph 3, it shall communicate the draft measure to the European Data Protection Board and the Commission [456].

3. The obligation set out in paragraph 2 shall apply to a draft measure (…) which:

454 SI scrutiny reservation. BE reservation on the time required for a consistency mechanism procedure. DE parliamentary reservation and ES reservation on the role of COM in the consistency mechanism.

455 DE thought that supervisory authorities of third countries for which there is an adequacy decision should be involved in the consistency mechanism; if third countries participated in the consistency mechanism, they would be bound by uniform implementation and interpretation.

456 IT proposed limiting this to cases where a coordination mechanism implemented by the lead authority does not result a solution acceptable to all supervisory authorities concerned.

(a) is intended to exercise the powers of the supervisory authority referred to in points (b), (c), (eb), (f), (g) and (h) of paragraph 1 of Article 53 or to impose an administrative fine pursuant to Articles 79 and 79a[457] and *relates to processing activities which substantially affect a significant number of*[458] *data subjects in several Member States; or*

(b) *may substantially affect the free movement of personal data within the Union*[459] [460]*;*

(c) *aims at adopting a list of the processing operations subject to the requirement for a data protection impact assesment pursuant to Article 33(2b); or*

(ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or

(cb) aims to approve the criteria for accereditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a;

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

457 IT suggested adding the sanctioning power under Article 79.

458 LU proposed adding 'a significant number'. PL and SE also thought the involvement of the EDPB should be confined to cases where the DPAs cannot agree among each others and referred in particular to paragraph 2(a). COM scrutiny reservation.

459 IT scrutiny reservation.

460 DE proposed combining (a) and (b) and thereby reducing the cases in which the consistency mechanism would need to be applied.

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

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

4. Any supervisory authority concerned[461] *or the European Data Protection Board may request that any matter referred to in paragraph 3 shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 3 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56*[462]*.*

5. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter referred to in paragraph 3 shall be dealt with in the consistency mechanism[463].

6. Supervisory authorities and the Commission shall electronically communicate to the European Data Protection Board[464]*, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, (…) the grounds which make the enactment of such measure necessary,* and the views of other supervisory authorities concerned.

461 BE, IT, SE SI and PL thought the scope of this paragraph should be limited so as to limit the number of cases. BE suggested deleting this paragraph

462 LU proposed restricting this to cases where the coordination mechanism implemented by the competent authority did not allow for a solution to be reached; ES referred to cases where the other authorities did not agree with the proposal of the competent(/lead) authority.

463 BE and DE asked for the deletion of this paragraph.

464 DE proposal.

7. *The chair of the European Data Protection Board shall <u>without undue delay</u>[465] electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The chair of the European Data Protection Board shall, where necessary, provide translations of relevant information.*

Article 58

Opinion by the European Data Protection Board

1. (…)

2. (…)

3. (…)

4. (…)

5. (…)

6. (…)[466]

7. The European Data Protection Board shall issue an opinion on matter<u>s submitted to it in the consistency mechanism referred to in Article 57 provided it has not already issued an opinion on the same matter</u>[467].

---

465 GR and IT suggestion.

466 Paragraphs 1 to 6 have been moved to Article 57.

467 ES suggested deleting the possibility for one DPA requesting an opinion from the EDPB, but keeping this possibility for the Commission.

7a. The opinion shall be adopted within one month[468] by simple majority of the members of the European Data Protection Board unless a supervisory authority of the Member State where a complaint has been lodged requests further consideration of the opinion. In that case the opinion shall be adopted by a two-third majority of the members of the European Data Protection Board[469].

7b. Where within the period referred to in paragraph 7a the European Data Protection Board does not adopt an opinion, the supervisory authority referred to in paragraph 2 of Article 57 may adopt its draft measure[470].

7c. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 2 and 4 of Article 57 and the Commission (…) of the opinion and make it public.

8. The supervisory authority referred to in paragraph 2 of Article 57 (…) shall take utmost[471] account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion , electronically communicate to the chair of the European Data Protection Board (…) whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

9. Where the supervisory authority concerned does not intend to follow the opinion, it shall inform the chair of the European Data Protection Board and the Commission within the period referred to in paragraph 8 and shall explain its refusal to follow the opinion[472].

---

468 BE and GR proposed two months.
469 DE proposed providing a mechanism for consultation of stakeholders.
470 Further to LU proposal.
471 Further to IT suggestion.
472 Further to DE proposal.

Article 59

Opinion by the Commission[473]

(…)

Article 60

Suspension of a draft measure[474]

(…)

473 Deleted in accordance with the request from BE, CZ, DE, ES, FR, SE and UK. PT and PL scrutiny reservation. COM reservation on deletion.

474 Deleted at the suggestion of BE, CZ, DE, FR, IT, SE and UK. PT scrutiny reservation. COM reservation on deletion.

Article 61

Urgency procedure[475]

1. In exceptional circumstances, where the competent supervisory authority considers that there is an urgent need to act in order to protect rights and freedoms of data subjects, (…) *it may*, by way of derogation from the consistency mechanism referred to in Article 57, immediately adopt provisional measures pursuant to points (b), (c), (eb), (f), (g) and (h) of paragraph 1 of Article 53[476],with a specified period of validity. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the European Data Protection Board and to the Commission[477].

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

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

---

475 COM explained that he urgency procedure was an essential part of the consistency mechanism. The existence of an urgency procedure was welcomed by several delegations (DE, ES, IT, NL), but also gave rise to many questions. There was lack of clarity surrounding the criteria which could warrant the taking of provisional measures (DE, FR, PT), in particular by another DPA. The need to respect certain procedural guarantees (e.g. giving notice to the data controller) prior to the taking of provisional measures was emphasised by FR.

476 COM scrutiny reservation.

477 The conditions under which the EDPB needed to be informed also gave rise to questions (GR, ES). Com stated the obligation only existed in cross-border cases

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

Article 62[478]

Implementing acts

1. The Commission may adopt implemending acts of general application for:

   (a) ensuring the correct and uniform application of this Regulation (…) in relation to matters communicated by supervisory authorities pursuant to Article 57(3)(b) (…).

   (b) (…);

   (c) (…)

   (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 57(6) and (7) and in Article 58(5).

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

[478] COM reservation.

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

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

Article 63

Enforcement[479]

1. For the purposes of this Regulation, a (…)measure of a supervisory authority of one Member State which is compliant with the requirements of this Section shall be enforceable in all Member States concerned.

2. (…)[480]

479 EE and SI reservation.
480 COM scrutiny reservation on deletion.

SECTION 3

EUROPEAN DATA PROTECTION BOARD[481]

Article 64

***European Data Protection Board*[482]**

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

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor[483].

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

4. The Commission[484] shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative <u>without voting rights</u>. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

---

481 Several Member States (BE, DE, IT, PT) pleaded in favour of granting the EDPB the power to take legally binding decisions in the context of the consistency mechanism and do away with the proposed Commission power to intervene. It was argued that the DPAs should have the same independence vis-à-vis the Commission, as vis-à-vis the Member States' authorities. COM argued that it was legally impossible under the T(F)EU to confer such powers on the EDPB. ES was also opposed to granting the EDPB the power to take legally binding decisions.

482 The term 'Board' seems inappropriate and could be replaced by Committee

483 NO pleaded in favour of the participation of the associated States. COM replied that the modalities for such participation were provided for in the association agreement.

484 It pleaded in favour of also including the Council and the Parliament.

Article 65

Independence

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

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

Article 66

Tasks of the European Data Protection Board

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular[485]:

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

   (b) examine, on its own initiative or on request of one of its members[486] or on request of the Commission[487], any question covering the application of this Regulation and issue guidelines, recommendations and best practices (…) in order to encourage consistent application of this Regulation;

485 DE suggested adding the provision of an opinion on the level of data protection in third countries or international organisations

486 FR suggested that controllers be added here. However a controller can always ask 'its' DPA to submit a certain issue to the DPA.

487 Some Member States (IT, DE) thought that, if Commission requests were included here, a similar possibility for the Council and the Parliament should be provided.

(ba) draw up guidelines for supervisory authorities concering the application of measures referred to in points (e) to (h) of paragraph 1 of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a;

(c) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (ba);

(ca) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;

(cb) give the Commission an opinion on the level of protection in third countries or international organisations;

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

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

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

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

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

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

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

Article 67

Reports

1. The European Data Protection Board shall at regular intervals inform the Commission about (…) its activities.

2. *It shall draw up an annual report (…) regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

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

Article 68

Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its members unless a two-third majority is required pursuant to Article 58(7a).

2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. (…)[488].

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members (…).[489]

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable once[490].

488 DE thought that the majorities by which further decisions shall be taken should be established by the EDPB itself

489 COM reservation on deletion.

490 Further to BE proposal. NL thought that also the case where a chair or a deputy chairperson ceases to be a member of the European Data Protection Board[/Committee], should be addressed by the Regulation. However, this may be left to national law of the Member state concerned. COM scrutiny reservation.

Article 70

Tasks of the chair

1. The chair shall have the following tasks:

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

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

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

Article 71

Secretariat

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat[491].

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

[491] DE reservation on entrusting the EDPS with the EDPB secretariat. The risk of conflicts of interest of EDPS staff was also raised.

3. The secretariat shall be responsible in particular for:

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

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

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

(d) the translation of relevant information;

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

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

Article 72

Confidentiality[492]

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

2. Access to documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001.

[492] DE, EE, ES, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this.

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

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS[493]

Article 73

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation.

2. In the situation referred to in paragraph 1, the data subject shall have the right to mandate a body, organisation or association, which *has been properly constituted according to the law of a Member State* and whose objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf (…).

3. Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with the competent[494] supervisory authority (…) if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.[495].

493 FR and EE scrutiny reservation.
494 COM reservation on limitation to competent supervisory authority.
495 BE reservation.

Article 74

Right to a judicial remedy against a supervisory authority[496]

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

2. Without prejudice to any other administrative or non-judicial remedy, a data subject shall have the right to a judicial remedy (…) where the supervisory authority does not deal with a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged under Article 73.

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

4. (…)

5. (…)[497]

Article 75

Right to a judicial remedy against a controller or processor[498]

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

496 SI reservation.
497 COM reservation on deletion of paragraphs 4 and 5.
498 SI scrutiny reservation.

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

3. (…)

4. (…)

Article 76 [499]

Representation of of data subjects

1. The data subject shall have the right to mandate a body, organisation or association referred to in Article 73(2) to exercise the rights referred to in Articles 74 and 75 on his or her behalf.[500]

2. (…)

3. (…)

4. (…)

5. (…)[501]

499 EE, PT and SI scrutiny reservation.

500 DE parliamentary reservation; BE reservation.

501 COM scrutiny reservation on deletion of paragraphs 3 to 5.

Article 77

Right to compensation and liability

1. Any person who has suffered damage as a result of a processing operation which is non compliant with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Whithout prejudice to Article 24(2), where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

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

Article 78

Penalties

(…)[502]

[502] This Article was moved to Article 79b.

Article 79

General conditions for imposing administrative fines

1. Each supervisory authority shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation. Such fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Articles 53(1).

2. Administrative fines imposed pursuant to Article 79a shall in each individual case be effective, proportionate and dissuasive.

2a. The amount of the administrative fine in each individual case shall be fixed with due regard to the following:

(a) the nature, gravity and duration of the infringment having regard to the nature scope or purpose of the processing concerned;

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

(c) the number of data subjects affected by the infringement and the level of damage suffered by them;

(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;

(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuang to Articles 23 and 30;

(f) any previous infringements by the controller or processor;

(g) the financial situation of the controller or processor, including any financial benefits gained, or losses avoided, directly or indirectly from the infringement;

(h) the maner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) the level of co-operation with the supervisory authority during the investigation of the infringement.

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;

(k) whether a data protection officer has been designated;

(l) whether the controller or processor is a public authority or body;

(m) any other aggravating or mitigating factor applicable to the circumstances of the case.

3. (…)[503]

[3a. Where a representative has been designated by a controller pusuant to Article 25, the administrative fines may be imposed on the representative without prejudice to any proceedings which may be taken against the controller].

3b. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

[503] COM reservation on deletion; linked to reservation on Article 79a.

4. The exercise by a supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process

Article 79a

Administrative fines[504]

1. The supervisory authority may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] % of its total annual (…) turnover, on a controller who, intentionally or negligently:

(a) does not (…) respond within the period referred to in Article 12(2) to requests of the data subject;

(b) charges a fee (…) in violation of Article 12(4).

2. The supervisory authority may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total annual (…) turnover, on a controller or processor who, intentionally or negligently:

(c) does not provide the information, or (…) provides incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Articles 14 and 14a;

504 COM reservation on replacing 'shall' by 'may' and the deletion of amounts and percentages in paragraphs 1, 2 and 3.

(d) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19;

(e) (…);

(f) (…);

(g) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;

(h) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4).

(i) (…)

3. The supervisory authority may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total annual turnover, on a controller or processor who, intentionally or negligently:

(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;

(b) (…);

(c) (…);

(d) does not comply with the conditions in relation to (…) profiling pursuant to Article 20;

(e) does not (…) implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 (…) and 30;

(f) does not designate a representative in violation of Article 25;

(g) processes or instructs the processing of personal data in violation of (…) Articles 26;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;

(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);

(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).

(n) (…)

(o) (…)

4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.]

Article 79b

Penalties[505]

1. *For infringments of the provisions of this Regulation not listed in Article 79a Member States shall lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (…). Such penalties shall be effective, proportionate and dissuasive.*

2. *(…).*

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

505 This corresponds to Article 78 of the Commission proposal.

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

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.

Article 80b

Processing of national identification number

Member States may determine the conditions for the processing of a national identification number or any other identifier of general application. [506]

Article 81

Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

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

   (b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

[506] BE suggestion based on Article 8(7) of the 1995 Directive. COM reservation.

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

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 82

Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

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

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

Article 83

Processing for historical, statistical and scientific (…) purposes

1. (…) Personal data may be processed for historical, statistical or scientific (…) purposes only if:

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

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

1a. The provisions and exceptions for historical, statistical, and scientific purposes within the limits of this Regulation shall apply only on condition:

   (a) that the data on any particular individual are not processed to support measures or decisions with respect to that individual, and

(b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject[507].

2. Personal data processed for historical, statistical or scientific (…) purposes may be published or otherwise publicly disclosed (…) only if:

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

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

(c) the data subject has made the data public[508].

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

507 Text proposed by the Statistics Working Party in 10428/12. COM reservation.

508 NO thinks it is unclear whether the researcher according to paragraph 2 will need a new and separate legal ground for publishing material that has been collected for research purposes, even if the initial legal basis for processing specifically mentions publishing.

Article 84

Obligations of secrecy

1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

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

Article 85

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

CHAPTER X

DELEGATED ACTS AND IMPLEMENTING ACTS[509]

Article 86

Exercise of the delegation

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

2. The delegation of power referred to in (…) Article 8(3), Article 9, (…) , Article 39a(7), [Article 43(3)], (…), Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in (…) Article 8(3), (…) Article 39a(7), [Article 43(3)], (…) Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

509 COM reservation on the deletion of empowerments for delegated acts or implementing acts.

5. A delegated act adopted pursuant to (…) Article 8(3), Article 9(3), (…) Article 39a(7), [Article 43(3)], (…), Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Article 87

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

FINAL PROVISIONS

Article 88

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 89

Relationship to and amendment of Directive 2002/58/EC

1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2 Article 1(2) of Directive 2002/58/EC shall be deleted.

Article 90

Evaluation

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

Article 91

Entry into force and application

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

2. It shall apply from [*two years from the date referred to in paragraph 1*].

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

Done at Brussels,

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