Council of the European Union

Brussels, 19 December 2014
(OR. en)

15395/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 165
JAI 860
MI 965
DRS 167
DAPIX 167
FREMP 202
COMIX 604
CODEC 2222

NOTE

From:	Presidency
To:	Working Party on Information Exchange and Data Protection
No. prev. doc.:	11013/13 DATAPROTECT 78 JAI 496 MI 546 DRS 119 DAPIX 88 FREMP 85 COMIX 380 CODEC 1475
No. Cion doc.:	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 under the Italian Presidency. Regarding Articles 4 (points 19a and 19b), 51, 54a, 54aa, 54b and 54c the Presidency had also circulated alternative drafts, which are set out in 16974/14 DATAPROTECT 187.

All changes made to the original Commission proposal are underlined text; where text has been deleted, this is indicated by (…). Where existing text has been moved, this text is indicated in *italics*. Changes that were not yet fully discussed in DAPIX are marked in **bold underlining**.

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 actors, including 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 (…) 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. Regarding the processing of personal data for compliance with a legal obligation,[4] for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC Member States have several sector specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules. Within this margin of manoeuvre sector-specific laws that Member States have issued implementing Directive 95/46/EC should be able to be upheld.

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.

[4] AT, supported by SI, made a proposal for a separate Article 82b which would allow Member States to adopt specific private sector provisions for specific situations (15768/14 DATAPROTECT 176 JAI 908 MI 916 DRS 156 DAPIX 179 FREMP 215 COMIX 623 CODEC 2300). The Presidency thinks that the revised recital 8 read together with Article 1(2a) sufficiently caters for this concern.

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. (…).

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[5] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.

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

15) This Regulation should not apply to processing of personal data by a natural person in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities. However, this Regulation should (…) apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, and, for these purposes, the maintenance of public order, or the execution of criminal penalties and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/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 **(…),** 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 the judiciary in the performance of its judicial tasks, including its decision-making. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.

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, 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.

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. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an 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, unless information on deceased persons is related to an identified or identifiable natural person.

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[6].

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.

[6] 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.

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 concerning health should include (…) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject[7]; including 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 the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. 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.

[7] BE proposal.

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. (…)[8].

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.

[8] 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 the 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. (…)

31a) Wherever this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant the constitutional order of the Member State concerned, however such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights.

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.
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.

35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data.

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 specify the general conditions of the Regulation governing the lawfulness of data processing, 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 strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. (...) 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 archiving purposes in the public interest, or for statistical, scientific or historical (…) 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 as the context of their processing may create important risks for the fundamental rights and freedoms[9]. These data 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 processing is allowed in specific cases set out in this Regulation. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly be provided for where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

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.

[9] BE proposal.

(42a) (…) Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health-care services and ensuring continuity of health-care and cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (…).

(42b) The processing of special categories personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to suitable and specific measures so as to protect the rights and freedoms of individuals. 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.

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

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

45) If the data processed by a controller do not permit the controller to identify a natural person (…) the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. (…). However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.

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. *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.* 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 archiving purposes in the public interest, 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 (…), where the processing of personal data is carried out by automated means, the data subject should also be allowed to transmit the personal data concerning him or her, which he or she has provided to a controller, in a commonly used and machine-readable format to another controller.
This right should apply where the data subject provided the personal data based on his or her consent or in the performance of a contract. It should not apply where processing is based on another legal ground other than consent or contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of a official duty vested in the controller.

Where, in a certain set of personal data, more than one data subject is concerned, the right to transmit the data should be without prejudice to the requirements on the lawfulness of the processing of personal data related to another data subject in accordance with this Regulation. This right should also not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should in particular not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. (…)

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) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her and taken which is based solely on automated processing, *which produces legal effects concerning him or her* or significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' intended to create or use a profile, that is a set of data characterising a category of individuals to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements~~;~~. However, decision making based on such processing, including profiling, should be allowed when authorised[10] by Union or Member State law to which the controller is subject, including for fraud and tax evasion[11] monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit 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, to express his or her point of view, to get an explanation of the decision reached after such assessment[12] and the right to contest the decision.

Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.

58a) The creation and the use of a profile, i.e. a set of data characterising a category of individuals that is e applied or intended to be applied to a natural person as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.

---

10 BE suggested adding ' or recommended', with regard to e.g. ECB recommendations.
11 Further to MT suggestion.
12 Further to PL suggestion.

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, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection and public health. 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 obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation (…). These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.

60a) Such risks, of varying likelihood and severity, may result from 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 to the reputation, loss of confidentiality of data protected by professional secrecy, [breach of (…) pseudonymity][13], 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; (…).

60b) *The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a high risk. A high risk is a particular*[14] *risk of prejudice to the rights and freedoms of individuals* (…).

[13] The reference to the use of pseudonymous data in Chapter IV will in the future need to be debated in the context of a further debate on pseudonymising personal data.

[14] The use the word 'particular' was questioned by BE, CZ, ES and UK, which thought that this term does not express the seriousness of the risk in case of 'high' risk.

60c) Guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller [or processor], especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk for the rights and freedoms of individuals and indicate what measures may be sufficient in such cases to address such risk. (…)

61) The protection of the rights and freedoms of individuals 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. Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, 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 of their behaviour in the Union, (…) the controller should designate a representative, unless (…) *the processing it carries out is* **occasional and unlikely** *to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing* **or** the controller 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 by the controller.

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. (…) Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose**s** of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject.

The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.

64) (…)

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 (…) risks inherent to the processing and implement measures to mitigate those risk. 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 risk and the nature of the personal data to be protected. (…). In assessing data security risk, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, 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, particularity and severity of this risk. 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. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

67) A personal data breach may, if not addressed in an adequate and timely manner, result in (…) physical, material or moral damage to individuals such as loss of control over their personal data or limitation of (…) their rights, discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the 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 which may result in (…) physical, material or moral damage has occurred 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 rights and freedoms could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. (…). 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 (…) the need to mitigate an immediate risk of damage 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) (…) It must be ascertained 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 (…). The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

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 (…).

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 types of processing operations which are likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, *context* and purposes (…). Such types of processing operations may be those which, in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing[15].

[15] BE was opposed to the temporal reference in the last part of this sentence.

70a) In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, *context and* purposes of the processing and the sources of the risk, which should include in particular the envisaged measures, safeguards and mechanisms for mitigating that risk and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to (…) 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 and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high (…) risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk for the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. *The processing of (…) personal data irrespective of the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by professional secrecy (…), such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.*

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 would, despite the envisaged safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of individuals (…), and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted, prior to the start of the processing activities. Such high (…) risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of (…) damage or (…) interference with the rights and freedoms of the data subject. 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 tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of individuals.

74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

74b) A consultation with the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data (…), in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

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 risk likely to result from the processing for the rights and freedoms of individuals.

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 controllers, processors or other recipients in 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 controllers, processors in the same or[16] 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. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects[17].

---

16 DE scrutiny reservation, in particular about the application of the rules of place of purchase in relation to Article 89a.

17 FR requests the second sentence to be inserted in Article 89a. NL asked what was meant with the new text and considered that it was necessary to keep it, but its purpose and meaning should be clarified. DE and UK scrutiny reservation on the new text. EE asked whether if "*affect"* means that it was not contradictory or something else.

80) The Commission may (…) decide with effect for the entire Union that certain third countries, or a territory or a specified sector, such as the private sector or one or more specific economic sectors 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 a third country or of a territory or of a specified sector within a 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. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country.

81a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol *should be taken into account*. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations[18].

[18] DE, supported by NL, proposed 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). According to the position of DE, although those systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards.

81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26 (4) of Directive 95/46/EC. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any pertinent findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation.

82) The Commission may (…) recognise that a third country, or a territory or a specified 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. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

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 ad hoc 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. They should relate in particular to compliance with the general principles relating to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.

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 explicit consent, where the transfer is occasional 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 rules should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange (….) between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, for example in case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport (…) .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 vital interests, including physical integrity or life, if the data subject is incapable of giving consent.[19] In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission.

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. The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms of natural persons with respect to processing of their personal data. 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.

[19] FR referred to the situation of a recipient of the transfer who is a medical professional or has adduced provisions ensuring the respect of the data subject's right to privacy and medical confidentiality. PRES considers that this could be further addressed in the context of Chapter IX.

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. (…)

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 tasks 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[20]. Neither does it imply that supervisory authorities cannot be subjected to judicial review.

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.

[20] Text proposed 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 and/or the government or the head of State of the Member State or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure.
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.

95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, processing affecting data subjects on its territory or processing carried out by a controller not established in the European Union when targeting data subjects residing in its territory. This should include dealing with complaints lodged by a data subject, conducting investigations on the application of the Regulation, promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

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, this Regulation should oblige and empower the supervisory authorities to co-operate with each other and the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

96a) Where the processing of personal data *takes place* in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State.

(…)

96b) The lead authority should be competent to (…) **give legal effect to** measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process.

96c) The decision (…) should be taken jointly **by the lead supervisory authority and** (…) the other supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities (…) in the Union.

97) A supervisory authority should not act as lead supervisory authority in local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involving only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State.

The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities and bodies of a Member State. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or body is established.

98) (…)

99) 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 tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, particularly in cases of complaints from individuals, and to bring infringements of this Regulation to the attention of the judicial authorities and/or engage in legal proceedings. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities (…) should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in national procedural law, such as the requirement to obtain a prior judicial authorisation.

Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head or a member of the supervisory authority of a person authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to national procedural law.

100) (…)[21].

[21] Moved to recital 111.

101) Where the supervisory authority to which the complaint has been lodged is not the lead supervisory authority, the lead 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 lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of 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.

101a) The supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of the Regulation should seek an amicable settlement and, if this proves unsuccessful, exercise its full range of powers in cases where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities (…) of the controller or processor in the one single Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect (…) **or is not likely to substantially affect** data subjects in other Member States. **This should include specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; or to processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or that has to be assessed taking into account relevant legal obligations under national law.**

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 **(…) individuals in particular in the educational context**.

103) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. Where a supervisory authority requesting mutual assistance, in the case of no response of the requested supervisory authority within one month of receiving the request, adopts a provisional measure, such provisional measure should be duly justified and only of a temporary nature.

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.

104a)(…)[22]

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 adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States (…). 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.

[22] Merged with recital 110.

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. The European Data Protection Board should also be empowered to **settle disputes between supervisory authorities. For that purposes it should** issue**, with a two-third majority of its members,** binding **positions in clearly defined** cases where there are conflicting views among supervisory authorities **in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, notably whether there is an infringement of this Regulation or not** (…).

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 (…) lawfulness of a (…) measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the **cooperation** mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and 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) In order to promote the consistent application of this Regulation, the European Data Protection Board should be set up as an independent body of the Union. To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chairperson. 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 or his or her representative 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, in particular on the level of protection in third countries or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks

111) Every data subject should have the right to lodge a complaint with a supervisory authority, in 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, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. **The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The 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**. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

112) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a 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) Without prejudice to the right of natural or legal person to bring an action for annulment of decisions of the European Data Protection Board which have been notified to him or her before the Court of Justice of the European Union, each natural or legal person should have the right to an effective judicial remedy against a decision of a supervisory authority which produces legal effects concerning this person. Such decisions concern in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. The fact that a natural or legal person has not brought an action for the annulment of the European Data Protection Board's decisions before the Court of Justice of the European Union within the mandatory time-limit, does not bar that person from calling in question the lawfulness of that decision before the national courts at a later stage in particular in the context of judicial review of a supervisory authority's decision applying the European Data Protection Board's decision. In that context, where a national court considers that the European Data Protection Board's decision may be unlawful, it shall request the Court of Justice of the European Union a preliminary ruling concerning the validity of that European Data Protection Board's decision, in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[23]. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and shall be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts whose decisions may be subject to appeal under national law should endeavour to request a preliminary ruling concerning the interpretation of Union law including this Regulation, in particular where the case involves a data subject who has lodged a complaint with a supervisory authority located in a Member State other than the one where the controller or processor has its establishment.

[23] Case C-314/85.

113a) Where a court seized with a proceeding against a decision of a supervisory authority has reason to believe that proceedings concerning the same processing activities or the same cause of action are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized should stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if the latter has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

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. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law[24].

[24] COM scrutiny reservation.

118a) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation No 1215/2012 should not prejudice the application of such specific rules[25].

118b) 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. These criminal sanctions may also allow for the deprivation of the profits obtained through infringements 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.

---

25 COM and DE scrutiny reservation.

121) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data, with the right to freedom of expression and information, as guaranteed by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities, on co-operation and consistency. In case these exemptions or derogations differ from one Member State to another, the national law of the Member State to which the controller is subject should apply. 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. (…)

121a) *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 should be able to 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 public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary derogations from the rules of this regulation. The reference to public authorities and bodies should in this context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data*[26].

122) (…)[27].

123) (…)[28].

[26] Moved from recital 18.
[27] Moved to recital 42a.
[28] Moved to recital 42b.

124) National law or collective agreements **(including 'works agreements')**[29] may provide for *specific rules on 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, equality and diversity in the workplace , 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*.

125) The processing of personal data for historical, statistical or scientific (…) purposes and for archiving purposes **in the public interest** (…) should, in addition to the general principles and specific rules of this Regulation, in particular as regards the conditions for lawful processing, also comply with respect other relevant legislation such as on clinical trials. The further processing of personal data for historical, statistical and scientific purposes and for archiving purposes **in the public interest** (…) should not be considered incompatible with the purposes for which the data are initially collected and may be processed for those purposes for a longer period than necessary for that initial purpose (…). Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements and the rights to access, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for historical, statistical or scientific purposes and for archiving purposes (…) The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.

125a)(…)[30].

[29] DE proposal.
[30] Moved to recitals 126c and 126d.

125aa) By coupling information from registries, researchers can obtain new knowledge of great value when it comes to e.g. widespread diseases as cardiovascular disease, cancer, depression etc. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about long-term impact of a number of social conditions e.g. unemployment, education, and the coupling of this information to other life conditions. Research results obtained on the basis of registries provide solid, high quality knowledge, which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services etc.

In order to facilitate scientific research, personal data can be processed for scientific purposes subject to appropriate conditions and safeguards set out in Member State or Union law. Hence consent from the data subject should not be necessary for each further processing for scientific **purposes**.

125b) The importance of archives for the understanding of the history and culture of Europe" and "that well-kept and accessible archives contribute to the democratic function of our societies', were underlined by Council Resolution of 6 May 2003 on archives in the Member States[31]. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons.

Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide that personal data may be further processed for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes[32].

---

31 OJ C 113, 13.5.2003, p. 2.

32 CZ reservation.

Codes of conduct may contribute to the proper application of this Regulation, including when personal data are processed for archiving purposes in the public interest by further specifying appropriate safeguards for the rights and freedoms of the data subject[33]. Such codes should be drafted by Member States' official archives or by the European Archives Group. Regarding international transfers of personal data included in archives, these must take place without prejudice of the applying European and national rules for the circulation of cultural goods and national treasures.

126) Where personal data are processed for scientific purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, processing of personal data for scientific purposes should include fundamental research, applied research, privately funded research[34] 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. Scientific purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures[35].

[33] CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.
[34] AT and SE scrutiny reservation.
[35] CZ, DK, FI, FR, HU, MT, NL, PT, SE, SI and UK scrutiny reservation.

126a) Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

126b) For the purpose of consenting to the participation in scientific research activities in clinical trials (…) the relevant provisions of Regulation (EU) No. 536/2014 of the European Parliament and of the Council should apply.

126c) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. *Union law or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for guaranteeing statistical confidentiality.*

126d) *The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in conformity with the statistical principles as set out in Article 338(2) of the Treaty of the Functioning of the European Union, while national statistics should also comply with national law. 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*[36] *provides further specifications on statistical confidentiality for European statistics.*

[36] 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. This is without prejudice to existing Member State obligations to adopt professional secrecy where required by Union law.

128) This Regulation respects and does not prejudice the status under **existing constitutional** 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. (...).

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

130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[37]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

[37] 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) (…)[38].

139) (…)[39]

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

[39] 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.

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

2a. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations as provided for in Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX[40].

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data[41].

[40] AT, CZ, HU, SI and SK reservation; these delegations were in favour of a minimum harmonisation clause for the public sector. LU reservation: this offers too much leeway.

[41] DK, FR, NL, SI scrutiny reservation.

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[42].

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[43], **safeguarding of public security**[44], or the execution of criminal penalties

3. (…).

---

[42] 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'.

[43] BE reservation on the terms 'for these purposes'.

[44] This change in wording will need to be discussed, but the Presidency has suggested this change in order to align the text to the suggested text in the Data Protection Directive for police and judicial cooperation.

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[45].

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.

[45] 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[46] 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) **(…)**

(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[47];

(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future[48];

---

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

47 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.

48 RO scrutiny reservation.

(3b) 'pseudonymisation' **means the** processing of **personal data in such a way that the data can** no longer **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.**

(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[49];

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

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; **[50]**

(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;[51] however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients**[52]**;

---

49 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).

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

51 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.

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

(8) 'the data subject's consent' means any freely-given, specific and informed (…)[53] 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[54];

(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[55];

(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[56] unique identification of that individual, such as facial images, or dactyloscopic data[57];

---

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

54 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.

55 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.

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

57 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.

(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[58];

(12a) 'profiling' means **a** form of automated processing of personal data intended to **(…)** use a profile **to evaluate** personal aspects relating to a natural person, in particular **to analyse and predict** aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements[59];

(12b) **'profile' means a set of data characterising a category of individuals that is intended to be applied to a natural person;**

(13) 'main establishment' means[60]

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes (…) and means of the processing of personal data are taken in **another** establishment of the controller in **the Union,** In this case the **establishment having taken such decisions** shall be considered as the main establishment. If no decisions as to the purposes (…) and means of the processing of personal data are taken in the Union, (…) the establishment of the controller in the Union where the main processing activities (….) take place;

---

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

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

60 DE, supported by AT, remarked that, in view technological developments, it was very difficult to pinpoint the place of processing and that it was very tricky to establish a main establishment with far-reaching legal consequences. EE also thought more clarity was required. DE, CZ, SI and PL expressed a preference for a formal criterion, which referred to the incorporation of the controller.

- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place;

- Where the controller exercises also activities as a processor, (…) the main establishment of the controller shall be considered as the main establishment for the supervision of processing activities;

- 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[61];

[61] DE scrutiny reservation. UK scrutiny reservation on all definitions in paragraphs 10 to 16.

(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[62] or group of enterprises engaged in a joint economic activity;

(18) (…)[63]

(19) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 46;

(19a) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing, because the controller or processor is established on the territory of the Member State of that supervisory authority or because data subjects residing in this Member State are **or likely to be** substantially affected by the processing.

(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[64] [65] [66].

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries[67];

---

62 DE queried whether BCRs could also cover intra-EU data transfers. COM indicated that there was no need for BCRs in the case of intra-EU transfers, but that controllers were free to apply BCRs also in those cases.

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

64 OJ L 204, 21.7.1998, p. 37–48.

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

66 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'.

67 NL queried whether MOUs would also be covered by this definition; FI queried whether Interpol would be covered. CZ, DK, LV, SI, SE and UK pleaded in favour of its deletion.

CHAPTER II

PRINCIPLES

Article 5

Principles relating to personal data processing

1. Personal data must be:

(a) processed lawfully, fairly[68] 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 personal data for archiving purposes **in the public interest**, for statistical, scientific or historical purposes shall not be considered incompatible with the initial purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…)[69];

(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;

---

[68] DE thought this concept should be detailed; COM pointed out this was already done in recital 30.

[69] 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 solely for archiving purposes **in the public interest**, for statistical, scientific or historical purposes purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject[70];

(ee) processed in a manner that ensures appropriate security (…) of the personal data.

(f) (…)[71]

2. The controller shall be responsible for compliance with paragraph 1[72].

Article 6

Lawfulness of processing[73]

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[74]consent to the processing of their personal data for one or more specific purposes[75];

(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;

---

70 IE proposal so as to cover all the safeguards required under the Regulation, including those in Chapter IV.

71 AT wondered whether a principle of digital autonomy should be added here.

72 It was previously proposed to add '*also in case of personal data being processed on its behalf by a processor*', but further to suggestion from LU and FR, this rule on liability may be dealt with in the context of Chapter VIII.

73 DE, AT, PT, SI, SE and SK scrutiny reservation.

74 FR, PL and COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'; UK thought that the addition of 'unambiguous' was unjustified.

75 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;

(d) processing is necessary in order to protect the vital interests of the data subject (…)[76];

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

(f) processing is necessary for the purposes of the legitimate interests[77] pursued by the controller or by a third party [78] 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][79] [80].

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

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

(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.

---

[76] BG scrutiny reservation; UK preferred the wording of the 1995 Directive.
[77] FR scrutiny reservation.
[78] Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, SE, SK and UK.
[79] BE, DK, MT SI, PT and UK had suggested deleting the last sentence. FR scrutiny reservation.
[80] 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.

This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing **by** the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.

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[81]:

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

(b) the context in which the data have been collected;

(c) the nature of the personal data;

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

(e) the existence of appropriate safeguards[82].

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) [83] of paragraph 1[84 85 86].

---

81 DK, FI, NL, SI and SE stressed the list should not be exhaustive. PT: add consent.

82 BG, DE and PL reservation: safeguards as such do not make further processing compatible.

83 DK, ES, FR and NL thought (f) should be added.

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

85 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'.

86 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.'

5. (…)

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous[87] 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. (…).

[87] 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 [88]

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child[89], the processing of personal data of a child below the age of 13 years[90] 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[91].

---

88 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

89 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.

90 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).

91 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(…)[92].

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)][93].

Article 9

***Processing of special categories of personal data*[94]**

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (…) shall be prohibited.[95]

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

(a) the data subject has given explicit consent to the processing of those personal data (…), except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

---

92 ES, FR and SE scrutiny reservation.

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

94 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. There appeared to be 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 pleaded in favour of the inclusion of national identifier.

95 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.

(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 or a collective agreement[96] in so far as it is authorised by Union law or Member State law providing for adequate safeguards[97]; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

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

(e) the processing relates to personal data which are manifestly made public[98] by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims[99]; or

---

96 FI proposal; there are normally rights and obligations given to both parties when processing personal data. In the employment context rights and obligations derives from law and also from collective agreements which are based normally on legislation

97 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.

98 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).

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

(g) processing is necessary for the performance of a task carried out for (…)[100] reasons of public interest, on the basis of Union law or Member State law which shall[101] provide for suitable and specific[102] measures to safeguard the data subject's legitimate interests; or

(h) processing (...) is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee[103], medical diagnosis, the provision of care or treatment or the management of health-care systems and services (…) on the basis of Union law or Member State law [104] and subject to the conditions and safeguards referred to in paragraph 4[105];

(ha) *processing of genetic data is necessary for (...) medical purposes*[106] and subject to the conditions and safeguards referred to in paragraph 4;

---

100 The term 'important' was deleted further to remarks by CZ, ES, FR, NL and UK.

101 NL suggested 'may'.

102 NL proposal.

103 FI proposal.

104 COM, ES, IE, PL scrutiny reservation.

105 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.

106 Some delegations wanted to deleted this point in its entirety: FR, SI. NL and UK wanted to include also criminal purposes ('*the performance of a task carried out by competent authorities on the basis of Union or Member State law for the purpose of prevention, investigation, detection or prosecution of criminal offences'*), but the Presidency thinks this is covered by the draft Directive. Should this not be the case, this point would indeed need to be amended.

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

(i) processing is necessary for archiving purposes **in the public interest** (…), historical, statistical or scientific (…) purposes and subject to the conditions and safeguards referred to in Article 83 (...) [or is necessary for studies conducted in the public interest in the area of public health][107].

(j) (...)[108]

2a. (…)[109]

3. (…)

4. *Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in points (h) and (ha) of paragraph 2 when (...) those data are processed by a* ***(…)*** *professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies to the obligation of professional secrecy*[110]*, or by another person also subject to an (...)obligation of secrecy under Member State law or rules established by national competent bodies.*

---

[107] Further to FR proposal. IE thought this was already covered by scientific research.

[108] NL and DE proposed adding "*insurance and reinsurance, in particular the conclusion and the performance of insurance contracts, the processing of statutory claims, the evaluation of risks, the establishment of tariffs, compliance with legal obligations and the combating of insurance fraud*". This was however viewed critically by AT, BE, EE, ES, FR, LU, PT, FI and UK.

[109] Moved to Article 9a.

[110] See clarification of the term professional secrecy in recital 122. PL would have preferred to refer to legal obligations, but some of the may not be laid down in (statutory) law. RO on the contrary thought it sufficient to refer to ' rules established by national competent bodies in the field of professional secrecy'.

4a. In case a transfer of personal data referred to Article 44(1)(f) involves personal data concerning health such transfer can take place only subject to the condition that those data will be processed by a health professional subject to the obligation of professional secrecy under the law of the third State concerned or rules established by national competent bodies to the obligation of professional secrecy, or by another person also subject to an (…) obligation of secrecy under the law of the third State concerned or rules established by national competent bodies[111].

Article 9a

Processing of data relating to criminal convictions and offences [112]

Processing of data relating to criminal convictions and offences or related security measures[113] *may only be carried out either under the control of official authority (...)*[114] *or when the processing is* based on points (c) and (e) of Article 6(1) *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[115]. A complete register of criminal convictions may be kept only under the control of official authority[116].

3. (…)

---

111 COM, CZ and FI reservation; EE and UK scrutiny reservation. FR proposed also to add an obligation of pseudonymisation.

112 The Presidency suggests putting this as a separate article, given the fact that Member States do not want to treat these data as sensitive data. EE reservation: under its constitution all criminal convictions are mandatorily public.

113 Addition suggested so as to clarify that this is without prejudice to the use of other legal bases (such as consent). This may allay the concerns raised in this regard by NL and DK.

114 This wording has been deleted as it merely repeated points c) and e) of Article 6(1).

115 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.

116 SE scrutiny reservation. UK reservation on last sentence.

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (…) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (…) this Regulation.[117].

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[118].

[117] AT, DE, FR, HU and UK scrutiny reservation.

[118] 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[119]

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[120]

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[121]. 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[122]. (…)

---

119 General scrutiny reservation by UK on the articles in this Chapter.
120 DE, SE, SI and FI scrutiny reservation.
121 COM reservation on deletion.
122 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[123] (…). 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 (…)[124] *manifestly* unfounded or excessive, in particular because of their repetitive character, the controller (…) may refuse to act on[125] the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request[126].

---

123 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.

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

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

126 IT scrutiny reservation.

4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

5. (…)

6. (…)

Article 13

Rights in relation to recipients

(...)

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14

Information <u>to be provided where the data are collected from the data subject</u>[127]

1[128]. Where personal data relating to a data subject are collected <u>from the data subject</u>, the controller shall (…), <u>at the time when personal data are obtained</u>, 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<u>; the controller may also include the contact details</u> of the data protection officer<u>, if any</u>;

(b) the purposes of the processing for which the personal data are intended (…);

---

127 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.

128 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[129] provide the data subject with such further information [130]necessary to ensure fair and transparent processing in respect of the data subject[131], having regard to the specific circumstances and context in which the personal data are processed[132]:

(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[133];

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

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data (…)[134];

---

129 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.

130 CZ suggested adding the word 'obviously'.

131 FR scrutiny reservation.

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

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

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

(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[135]; and

(h) *the existence of* **automated decision making including** *-profiling referred to in Article 20(1) and (3) and information concerning* (…) *the* ***processing*** *, as well as the significance and the envisaged consequences of such* ***processing*** *for the data subject*.[136]

2. (…)[137]

3. (…)

4. (…)

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

6. (…)

7. (…)

8. (…)

[135] CZ, DE, ES and NL reservation.
[136] SE scrutiny reservation.
[137] 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[138]

1[139]. 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[140] 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;

---

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

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

140 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[141];

*(h) the existence of **automated decision making including** profiling referred to in Article 20(1) and (3) and information concerning (...) the **processing**, as well as the significance and the envisaged consequences of such **processing** for the data subject.*[142]

3. The controller shall provide the information referred to in paragraphs 1 and 2[143]:

(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.

---

141 COM and AT scrutiny reservation.

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

143 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 **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing[144]; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[145]; 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[**146**]; or

(d) where the data originate from publicly available sources[147]; or

(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person[148].

5. (…)

6. (…)

---

144 COM scrutiny reservation.

145 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.

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

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

148 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.

Article 15

Right of access for the data subject[149]

1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge[150] (…) 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[151];

   (b) (…)

   (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries[152];

   (d) where possible, the envisaged[153] 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;

---

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

150 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.

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

152 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.

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

(f) the right to lodge a complaint to a supervisory authority (…)[154] [155];

(g) where the personal data are not collected from the data subject, any available information as to their source[156];

(h) in the case of **automated decision making including profiling** referred to in Article **20(1) and (3)**, knowledge of the logic involved[157] in any automated data processing as well as the significance and envisaged consequences of such processing[158].

1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer[159].

1b. On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.

---

154 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.

155 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.

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

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

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

159 FR and UK scrutiny reservation on links with Chapter V

2. Where personal data supplied by the data subject are processed by automated means and in a structured and commonly used format, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject in that format to the data subject[160].

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 **[161]**

3. (…)

4. (…)

5. **(…)**[162]

[160] 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.

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

[162] Deleted in view of the new articles 83a to 83c.

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[163]

1. (…) The data subject shall have the right[164] 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. **(…)**[165]

---

163 DE and UK scrutiny reservation.

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

165 Deleted in view of the new articles 83a to 83c

Article 17

Right to be forgotten and to erasure[166]

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

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

[166] 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).

(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[167];

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[168] [169].

2. (…).

---

167 UK scrutiny reservation: this was overly broad.

168 RO scrutiny reservation.

169 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.

2a. *Where the controller[170] (...) has made the personal data public[171]* *and is obliged pursuant to paragraph 1 to erase the data,* the controller, taking account of available technology and the cost of implementation[172], *shall take (...) reasonable steps[173], including technical measures, (...) to inform controllers[174] which are processing* the *data, that a data subject requests them to erase any links to, or copy or replication of that personal data[175].*

---

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

171 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.

172 Further to NL suggestion. This may hopefully also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;

173 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.

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

175 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[176] 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[177];

b. for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject[178] or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[179];

c. for reasons of public interest in the area of public health in accordance with Article 81[180];

d. for archiving purposes in the public interest or for historical, statistical and scientific (…) purposes in accordance with **Article 83**;

e. (…)

f. (…)

g. for the establishment, exercise or defence of legal claims.

---

176 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.

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

178 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).

179 AT scrutiny reservation.

180 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.

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[181];

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

   (c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. (…)

3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest[182].

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

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

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[183].

5. (…)

5a. **(…)**[184]

Article 17b

Notification obligation regarding rectification, erasure or restriction[185]

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

---

183 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.

184 Deleted in view of the new articles 83a to 83c.

185 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.

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

Article 18

Right to data portability[187]

1. (…)

2. **T**he data subject shall have the right to **transmit the personal data**[188] **concerning him or her which he or she has provided to a controller to another controller** in a commonly used[189] **and**[190] **machine-readable** format without hindrance from the controller **to which the data have been provided to**, where
(a) **the processing is based on** consent or on a contract **pursuant to points (a) and (b) of Article 6 (2) or point (a) of Article 9 (2); and**

---

187 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. NL and CZ thought its scope should be limited to social media. 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, FI, SE and UK also underscored 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). DE, ES, FR, HU, IE and PL were in principle 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. BE, CZ and RO thought that the exclusion of the public sector should be mentioned not only in recital 55, but also here (ES was opposed thereto).

188 PL suggested to specify that this pertained to personal data in their non-aggregated or non-modified form. DE also queried about the scope of this right, in particular whether it could extend to data generated by the controller or data posted by third persons.

189 DE and FI queried whether this meant the scope was restricted to currently used formats (excluding future developments) and whether it implied an obligation for controllers to use one of these commonly used formats.

190 PT thought 'and' should be deleted.

(b) **the** processing is carried **out by automated means**[191]**.**

2a. The exercise of this right shall be without prejudice to Article 17.

2aa. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights in relation to the processing of the **those personal** data[192].

[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).] [193]

4. (…)[194].

---

191 BE, DE, ES, IE, FI and FR these delegations thought emphasis should be put on the right to withdraw data, also with a view to creating an added value as compared to the right to obtain a copy of personal data. VY and HU also thought the obligation of the controller should be emphasised.

192 ES thought there should be an exception in case disproportionate efforts would be required.

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

194 Deleted in view of the new articles 83a to 83c.

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19

Right to object[195]

1. The data subject shall have the right to object, on reasoned[196] 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)[197]**;** 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[198].

---

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

196 COM reservation.

197 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.

198 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 (…)[199] process the personal data concerned except for the establishment, exercise or defence of legal claims[200].

2. Where personal data are processed for direct marketing[201] purposes, the data subject shall have the right to object (…) at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…) and shall be presented clearly and separately from any other information[202].

---

199 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'.

200 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.

201 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.

202 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. **(…)**[203]

Article 20

Profiling[204]

1. **The** data subject shall have the right not to be subject to a decision **evaluating personal aspects relating to him or her, which is** based solely **on automated processing, including** profiling**, and** *produces legal effects* concerning him or her or **significantly** [205] affects him or her.

---

203 Deleted in view of the new articles 83a to 83c, where - as is currently the case under Directive 95/46- no exception to Article 19 is provided.

204 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).

205 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).

1a. **A data subject may be subject to a decision] referred to in paragraph 1 only if it**

(a) is **necessary for** entering into, or performance of, a contract between the data subject and a data controller **(…)**[206]; or

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

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

1b. **In cases referred to in paragraph 1a) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision**[207];

2. (…)

3. **Decisions referred to in paragraph 1a** shall not (…) be based on special categories of personal data referred to in Article 9(1), unless **points (a) or (g) of** Article 9(2) **apply** and suitable measures to safeguard the data subject's legitimate interests [208] are in place.

4. (…)

5. (…)

---

206 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.

207 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.

208 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[209]

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 (…) Articles 12 to 20 and Article 32, as well as Article 5[210] in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

   (aa) national security;

   (ab) defence;

   (a) public security;

   (b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, safeguarding public security[211], or the execution of criminal penalties;

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

---

[209] 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. 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.

[210] AT reservation.

[211] The wording of points (b), and possibly also point (a), will have to be discussed again in the future in the light of the discussions on the relevant wording of the text of the Data Protection Directive for police and judicial cooperation.

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

(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 (aa), (ab), (a), (b), (c) and (d);

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

(g) the enforcement of civil law claims.

2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, 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, the storage periods and the applicable safeguards taking into account of the nature, scope and purposes of the processing or categories of processing and the risks for the rights and freedoms of data subjects.

CHAPTER IV

CONTROLLER AND PROCESSOR[212]

SECTION 1
GENERAL OBLIGATIONS

Article 22

Obligations of the controller

1. Taking into account the nature, scope context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. (…)

2a. Where proportionate in relation to the processing activities[213], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.

3. (…)

4. (…)

---

212 SI and UK scrutiny reservation on the entire chapter. BE, DE, NL and UK have not been not convinced by the figures provided by COM according to which the reduction of administrative burdens doing away with the general notification obligation on controllers, outbalanced any additional administrative burdens and compliance costs flowing from the proposed Regulation.

213 HU, RO 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.

Article 23

Data protection by design and by default

1. (…) Having regard to available technology and the cost of implementation and taking account of *the nature, scope, context and purpose**s** of the processing* as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation[214]], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary[215] for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

2a. An approved certification mechanism pursuant to Article 39 *may be used as an element* to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

3. (…)

4. (…)

---

214 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. This debate will however need to take place in the context of a debate on pseudonymising personal data.

215 CZ would prefer "not excessive". This term may be changed again in the future in the context of the debate on the wording of Article 5(1)(c).

Article 24

Joint controllers[216]

1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.

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.

3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights (…).

---

216 SI reservation; it warned against potential legal conflicts on the allocation of the liability and SI therefore thought this article should be further revisited in the context of the future debate on Chapter VIII. FR also thought the allocation of liability between the controller and the processor is very vague and CZ expressed doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings and thought it should contain a safeguard against outsourcing of responsibility.

Article 25

Representatives of controllers not established in the Union

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

2. This obligation shall not apply to:

   (a) (…); or

   (b) *processing which is* occasional[217] and *unlikely to result in a* (…) *risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing* (…); or

   (c) a public authority or body;

   (d) (…)

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

3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.

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

[217] HU, SE and UK reservation.

Article 26

Processor

1. (…).[218] The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…).

1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes[219].

1b. (…)[220].

2. The carrying out of processing by a processor shall be governed by a contract or **a** legal act under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the rights of the controller (…) and stipulating, in particular that the processor shall:

(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;

---

218 The Presidency suggest completing Article 5(2) with the words "also in case of personal data being processed on its behalf by a processor". This may also need further discussion in the context of the future debate on liability in the context of Chapter VIII.

219 LU and FI were concerned that this might constitute an undue interference with contractual freedom.

220 Several delegations (CZ, AT, LU) pointed to the need to align this with the rules in Article 77. The discussion on the exercise of data subjects rights should indeed take place in the context of Chapter VIII.

(b) (…)

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

(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;

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

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

(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;

(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller.

The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.

2a. Where a processor enlists (…) another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law*[221], in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved *certification mechanism pursuant to Article 39*[222] may be used as an element to demonstrate *sufficient guarantees referred to in paragraphs 1 and 2a.*

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.

---

221 HU suggested qualifying this reference to EU or MS law by adding 'binding that other processor to the initial processor'.

222 FR reservation; SK suggested specifying that where the other processor fails to fulfil its data protection obligations under such contract or other legal act, the processor shall remain fully liable to the controller for the performance of the other processor's obligation. By authorising the processor to subcontract itself and not obliging the sub-processor to have a contractual relationship with the controller, it should ensure enough legal certainty for the controller in terms of liability. The principle of liability of the main processor for any breaches of sub-processor is provided in clause 11 of Model clause 2010/87 and BCR processor and is therefore the current standard. It also suggested deleting the reference to Article 2aa.

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2) [223].

2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.

4. (…)

5. (…)[224]

Article 27

Processing under the authority of the controller and processor

(…)

[223] PL was worried about a scenario in which the Commission would not act. CY and FR were opposed to conferring this role to COM (FR could possibly accept it for the EDPB).

[224] COM reservation on deletion.

Article 28

Records of categories of personal data processing activities[225]

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

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

   (b) (…)

   (c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f);

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

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

   (f) where applicable, the categories of transfers of personal data to a third country or an international organisation (…);

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

   (h) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

[225] AT scrutiny reservation.

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

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;

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

(c) the categories of processing carried out on behalf of each controller;

(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.

3. On request, the controller and the processor and, if any, the controller's representative, shall make the record available (…) to the supervisory authority.

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

(a) (…); or

(b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject such as (…) discrimination, identity theft or fraud, [breach of (…) pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or

5. (…)

6. (…)

Article 29

Co-operation with the supervisory authority

(…)

SECTION 2
DATA SECURITY

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures[, including **(…)** pseudonymisation of personal data] to ensure a level of security appropriate to the risk.

1a. In assessing the appropriate level of security account shall be taken in particular of the risk**s** that are presented by data processing (…), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. (…)

2a. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to *demonstrate compliance with the requirements set out in paragraph 1.*

2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3. (…)

4. (…)

Article 31

Notification of a personal data breach to the supervisory authority[226]

1. In the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

1a. The notification referred to in paragraph 1 shall not be required if a communication to the data subject is not required under Article 32(3)(a) and (b)[227].

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

---

226 AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded; SI thought this alignment could be achieved by deleting "high" before "risk" in Articles 31 and 32.

227 AT and PL thought this paragraph should be deleted.

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 approximate categories and number of data subjects concerned and the categories and approximate number of data records concerned;

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

(c) (…)

(d) describe the likely consequences of the personal data breach identified by the controller;

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

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.

4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. (…).

5. (…)

6. (….)[228]

228 COM reservation on deletion.

Article 32

Communication of a personal data breach to the data subject[229]

1. When the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall (…) communicate the personal data breach to the data subject without undue delay.

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

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

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

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

[229] AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or

d. it would adversely affect a substantial public interest.

4. (…)

5. (…)

6. (…)[230]

[230] COM reservation on deletion.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 33

Data protection impact assessment [231]

1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high[232] risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of **(…)** pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller (…)[233] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…).

---

231 FR, HU, AT and COM expressed doubts on the concept of new types of processing, which is now clarified in recital 70. UK thought this obligation should not apply where there is an overriding public interest for the processing to take place (such as a public health emergency).

232 FR, RO, SK and UK warned against the considerable administrative burdens flowing from the proposed obligation. The UK considers that any requirements to carry out a data protection impact assessment should be limited to those cases where there is an identified high risk to the rights of data subjects.

233 COM reservation on deletion.

1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[234] are based that produce legal effects concerning data subjects or severely affect data subjects;

(b) processing of special categories of personal data under Article 9(1) (…)[235], biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale ;

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

(d) (…);

(e) (…)[236].

2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board. [237]

234 In the future this wording will be aligned to the eventual wording of Article 20.

235 HU suggested that data pertaining to children be also reinserted.

236 FR scrutiny reservation. PL thought a role could be given to the EDPB in order to determine high-risk operations.

237 CZ reservation.HU wondered what kind of legal consequences, if any, would be triggered by the listing of a type of processing operation by a DPA with regard to on-going processing operations as well as what its territorial scope would be. In the view of the Presidency any role for the EDPB in this regard should be discussed in the context of Chapter VII.

2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.

2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [238]

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1, the measures envisaged to address the risk including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned[239].

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment[240].

4. *The controller shall seek the views of data subjects or their representatives on the intended processing,* without prejudice to the protection of commercial or public interests or the security of the processing operations (…)[241].

---

238 CZ reservation.
239 FR scrutiny reservation.
240 HU thought this should be moved to a recital.
241 CZ and FR indicated that this was a completely impractical obligation; IE reservation.

5. (…) 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, and such law regulates the specific processing operation or set of operations in question[242], paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. (…)

7. (…)

Article 34

Prior (…) consultation[243]

1. (…)

2. The controller (…)[244] 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 would result in a high (…) risk in the absence of measures *to be taken by the controller* to mitigate the risk..

---

242 BE and SI stated that this will have to be revisited in the context of the future debate on how to include the public sector in the scope of the Regulation.

243 HU scrutiny reservation; SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

244 COM and LU reservation on deleting processor.

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 the controller has insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may use any of its powers referred to in[245] Article 53 (…). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.

4. (…)

5. (…)

6. When consulting the supervisory authority pursuant to paragraph 2, the controller (…) shall provide the supervisory authority, with

   (a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

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

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

   (d) where applicable , the contact details of the data protection officer;

   (e) the data protection impact assessment as provided for in Article 33; and

   (f) any (…) other information requested by the supervisory authority (…).

[245] UK reservation; it thought the power to prohibit processing operations should not apply during periods in which there is an overriding public interest for the processing to take place (such as a public health emergency). The Presidency thinks this issue should however be debated in the context of Chapter VI on the powers of the DPA, as these may obviously also be used regardless of any consultation.

7. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure adopted by a national parliament or of a regulatory measure based on such a legislative measure which provide for the processing of personal data (…)[246].

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[247].

8. (…)

9. (…)

[246] IE scrutiny reservation on deletion.
[247] 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,[248] designate a data protection officer (…).

2. A group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. (…).

5. The (…) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37, particularly the absence of any conflict of interests. (…).

6. (…)

7. (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.

---

248 Made optional further to decision by the Council. AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself and may want to revert to this issue at a later stage. COM reservation on optional nature and deletion of points a) to c).

8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority (…).

10. Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.

11. (…)

Article 36

Position of the data protection officer

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

2. The controller or the processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing (…) resources necessary to carry out these tasks as well as access to personal data and processing operations.

3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. He or she shall not be penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

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

Article 37

Tasks of the data protection officer

1. The (…) data protection officer (…) shall have 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 and other Union or Member State data protection provisions (…);

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;

(c) (…)

(d) (…)

(e) (…)

(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

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

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter.

2. (…)

2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the *nature, scope, context and purposes* of the processing.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct [249]

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.

1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(a) fair and transparent data processing;

(aa) the legitimate interests pursued by controllers in specific contexts;

(b) the collection of data;

(bb) the pseudonymisation of personal data;

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

(d) the exercise of the rights of data subjects;

(e) information and protection of children and the way to collect the parent's and guardian's consent;

(ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security of processing referred to in Article 30;

[249] AT, FI, SK and PL scrutiny reservation.

(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;

(f) (…).

1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct *approved* pursuant to paragraph 2 may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights**.**

1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory[250] monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct, or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

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 is approved, and if 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.

---

250 CZ preferred this monitoring to be optional.

2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards[251].

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, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards ,the European Data Protection Board shall submit its opinion to the Commission.

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

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

5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

[251] FR made a proposal for a paragraph 2c: 'Approved codes of conduct pursuant to paragraph 2a shall constitute an element of the contractual relationship between the controller and the data subject. When such codes of conduct determine the compliance of the controller or processor with this Regulation, they shall be legally binding and enforceable.'

Article 38a

Monitoring of approved codes of conduct[252]

1. Without prejudice to the tasks 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 (1b), may be carried out by a body[253] which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

2. A body referred to in paragraph 1 may be accredited for this purpose if:

   (a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

   (b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

   (c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;

   (d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

---

252 AT, LU scrutiny reservation.

253 CZ, ES, LU 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. Codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

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

Article 39

Certification[254]

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

254 AT, FR, FI scrutiny reservation. FR thought the terminology used was unclear an that the DPA should be in a position to check compliance with certified data protection policies; this should be clarified in Article 53.

1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks *approved* pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights

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 tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2a. A certification pursuant to this Article shall be issued *by the* certification *bodies referred to in Article 39a, or where applicable, by the competent supervisory authority* on the basis of the criteria approved by the competent supervisory authority or, *pursuant to Article 57*, the European Data Protection Board[255].

3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, *or where applicable, the competent supervisory authority,* with all information and access to its processing activities which are necessary to conduct the certification procedure.

4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority where the requirements for the certification are not or no longer met.

[255] This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

Article 39a

Certification body and procedure[256]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:

   (a) the supervisory authority which is competent according to Article 51 or 51a; and/or

   (b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.

2. The certification body referred to in paragraph 1 may be accredited for this purpose only 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;

   (aa) it has undertaken to respect the criteria *referred to in paragraph 2a of Article 39* and approved by the supervisory authority which is competent according to Article 51 or 51a or , pursuant to Article 57, the European Data Protection Board;

[256] AT, FR, LU scrutiny reservation.

(b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;

(b) 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;

(c) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, *pursuant to Article 57*, the European Data Protection Board[257]. *In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies*.

4. The certification body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.

5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

[257] This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

6. *The* requirements referred to in paragraph 3*, the* criteria referred to in paragraph 2a of Article 39 *shall be made public by the supervisory authority in an easily accessible form*. The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification 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[258].

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].

7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7[259].

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)[260].

---

258 CZ, FR and HU though the national accreditation body should always consult the DPA before accrediting a certification body.

259 This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

260 DE pleaded in favour of deleting the last two paragraphs and suggested adding a new paragraph: "The previous paragraphs shall not affect provisions governing the responsibility of national certification bodies, the accreditation procedures and the specification of criteria for security and data protection. Commission's power to adopt acts pursuant to paragraphs 7 and 8 shall not apply to national and international certification procedures carried out on this basis. Security certificates issued by the responsible bodies or bodies accredited by them in the framework of these procedures shall be mutually recognized." ES also thought that this should not be left exclusively to the Commission.

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[261] [262] [263] [264]

Article 40

General principle for transfers

(…)

---

261 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, 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. FR and DE asked whether a transfer of data in the context of cloud computing or the disclosure of personal data on the internet constitutes an international transfer of data. DE also thought that the Regulation should create a legal framework for 'Safe Harbor-like' arrangements under which certain guarantees to which companies in a third country have subscribed on a voluntary basis are monitored by the public authorities of that country. 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 (FR, PL).

262 NL and UK pointed out that under the 1995 Data Protection Directive the controller who wants to transfer data is the first one to assess whether this possible in under the applicable (EU) law and they would like to maintain this basic principle, which appears to have disappeared in the Commission proposal.

263 DE asked which law would apply to data transferred controllers established in third countries that come within the ambit of Article 3(2); namely whether this would be EU law in accordance with that provision.

264 AT has made a number of proposals regarding this chapter set out in 10198/14 DATAPROTECT 82 JAI 363 MI 458 DRS 73 DAPIX 71 FREMP 103 COMIX 281 CODEC 1351.

Article 41

Transfers with an adequacy decision[265]

1. A transfer of personal data to **(...)** a third country or an international organisation may take place where the Commission[266] has decided that the third country, or a territory or one ore more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…)[267], both general and sectoral, 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 third country or international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…)[268];

---

265 Some delegations raised concerns on the time taken up by adequacy procedures and stressed the need to speed up this process. COM stated that this should not be at the expense of the quality of the process of adequacy.

266 CZ, DE 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.

267 AT would have preferred including a reference to national security.

268 NL thought that Article 41 was based on fundamental rights and legislation whereas Safe harbour is of a voluntary basis and that it was therefore useful to set out elements of Safe Harbour in a separate Article. DE asked how Safe Harbour could be set out in Chapter V.

(b) the existence and effective functioning of one or more independent supervisory authorities[269] in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;

(c) the international commitments the third country or international organisation concerned has entered into, or other (…) obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

2a. The European Data Protection Board shall give the Commission an opinion[270] for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.

[269] NL queried how strict this independence would need to be assessed. BE suggested adding a reference to independent judicial authorities, FI suggested to refer to 'authorities' *tout court*.

[270] CZ would prefer stronger language on the COM obligation to request an opinion from the EDPB.

3. The Commission, after assessing the adequacy[271] of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…)**[272]. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies) mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2)[273].

3a. *Decisions adopted by the Commission on the basis of Article 25(6)* **(…)** *of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[274] in accordance with the examination procedure referred to in Article 87(2)[275].

---

271 CZ, RO and SI reservation on giving such power to the Commission. DE thought that stakeholders should be involved in this process. 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.

272 CZ, DE, DK, HR, IT, NL, PL, SK and RO thought an important role should be given to the EDPB in assessing these elements.COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

273 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.

274 Moved from paragraph 8. CZ and AT thought an absolute maximum time period should be set (sunset clause), to which COM was opposed. NL, PT and SI thought this paragraph 3a was superfluous or at least unclear. Also RO thought that, if maintained, it should be moved to the end of the Regulation.

275 DE and ES suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011. DE asked if a decision in paragraph 3a lasted forever. IE considered paragraph 3a providing necessary flexibility. CZ thought that new States should not be disadvantaged compared to those having received an adequacy decision under Directive 1995.

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[276].

5. The Commission may decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer 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)[277]. **(…)**

5a. 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.

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44[278].**(…)**

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

8. (…)

---

276 BE queried about the reference to the 1995 Directive. CZ perceives this as superfluous.

277 FR and UK suggested the EDPB give an opinion before COM decided to withdraw an adequacy decision.

278 DE asked for the deletion of paragraph 6. DK thought the moment when third countries should be consulted was unclear.

Article 42

Transfers by way of appropriate safeguards[279]

1. In the absence of a decision pursuant to paragraph 3 of Article 41, a controller or processor may transfer personal data to (…) a third country or an international organisation only if the controller or processor has adduced appropriate safeguards, also covering onward transfers (…).

2. The appropriate safeguards referred to in paragraph 1 *may* be provided for (…), without requiring any specific authorisation from a supervisory authority, by:

   (oa) a legally binding and enforceable instrument between public authorities or bodies[280]; or

   (a) binding corporate rules referred to in Article 43; or

   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2)[281]; or

   (c) standard data protection clauses adopted by a supervisory authority (….) and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2).

   (d) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, including as regards data subjects' rights ; or

---

279 UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of these procedures regarding data flows in the context of cloud computing was also questioned.

280 HU has serious concerns; the proposed general clause ("a legally binding instrument") is too vague because the text does not define its content. Furthermore, the text does not provide for previous examination by the DPA either. HU therefore suggests either deleting this point or subjecting such instrument to the authorisation of the DPA, as it believes that there is a real risk that transfers based on such a vague instrument might seriously undermine the rights of the data subjects.

281 FR reservation on the possibility for COM to adopt such standard clauses.

(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

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

(b) (…)

(c) (…)

(d) provisions to be inserted into administrative arrangements between public authorities or bodies (…).

3. (…)

4. (…)

5. (…)

5a. The supervisory authority shall apply the consistency mechanism in the cases referred to in points (ca), (d), (e) and (f) of Article 57 (2).

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*[282]. *Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[283] in accordance with the examination procedure referred to in Article 87(2)[284].

---

282 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. DE emphasised the need of monitoring.

283 AT thought an absolute time period should be set.

284 DE and ES have suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

Article 43

Binding corporate rules[285]

1. The competent supervisory authority shall *approve*[286] *binding corporate rules* in accordance with the consistency mechanism set out in Article 57 provided that they:
   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;
   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:
   (a) the structure and contact details of the *concerned* group and of each of its members;
   (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, (…) 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;

---

285 NL thought it should be given a wider scope. BE and NL pointed to the need for a transitional regime allowing to 'grandfather' existing BCRs. NL asked whether the BCRs should also be binding upon employees. SI thought BCRs 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. HU said that it thought that BCRs were used not only by profit-seeking companies but also by international bodies and NGOs.

286 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.

(e) the rights of data subjects in regard to the processing of their personal data 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;

(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[287];

(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 or any other person or entity in charge of the 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. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority;

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

[287] DE thought that the reference to exemptions should be deleted here.

(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[288];

(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules[289]; and

(m) the appropriate data protection training to personnel having permanent or regular access to personal data (...).

2a. The European Data Protection Board shall advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules.

[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.][290]

4. The Commission may specify the format and procedures for the exchange of information (…) 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).

---

288 BE suggested making this more explicit in case of a conflict between the 'local' legislation applicable to a member of the group and the BCR.

289 CZ expressed concerns about the purpose of this provision and its application. UK found this point very prescriptive and wanted BCRs to be flexible to be able to be used for different circumstances.

290 CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives. RO and HR thought the EDPB should be involved. PL and COM wanted to keep paragraph 3.

Article 44

Derogations for specific situations[291]

1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules (...), a transfer or a category of transfers of personal data to (…) a third country or an international organisation may take place only on condition that:

(a) the data subject has explicitly[292] consented to the proposed transfer, after having been informed that such transfers may involve *risks* for the data subject 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[293]; or

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

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

---

291 EE reservation. NL parliamentary reservation. CZ, EE and UK and other delegations that in reality these 'derogations' would become the main basis for international data transfers and this should be acknowledged as such by the text of the Regulation.

292 UK thought the question of the nature of the consent needed to be discussed in a horizontal manner.

293 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. IT reservation on the (subjective) use of the concept of public interest. HR suggested adding 'which is not overridden by the legal interest of the data subject'.

(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; or

(h) the transfer, *which* is not large scale or *frequent*[294], is necessary for the purposes of legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and (…) based on this assessment adduced suitable safeguards[295] with respect to the protection of personal data.

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

3. (…)

4. Points (a), (b), (c) and (h) of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers[296].

---

294 AT, ES, HU, MT, PL, PT and SI would prefer to have this derogation deleted as they think it is too wide; it was stated that data transfers based on the legitimate interest of the data controller and directed into third countries that do not provide for an adequate level of protection with regard to the right of the data subjects would entail a serious risk of lowering the level of protection the EU *acquis* currently provides for.) DE and ES scrutiny reservation on the terms 'frequent or massive'. DE, supported by SI, proposed to narrow it by referring to 'overwhelming legitimate interest'. ES proposed to replace it by 'are small-scale and occasional'; UK asked why it was needed to add another qualifier to the legitimate interest of the transfer and thought that such narrowing down of this derogation was against the risk-based approach.

295 AT and NL reservation: it was unclear how this reference to appropriate safeguards relates to appropriate safeguards in Article 42.

296 BE scrutiny reservation. FR has a reservation concerning the exception of public authorities.

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

5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation[297]. Member States shall notify such provisions to the Commission[298].

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 (…).

6a. (…)

7. (…)

Article 45

International co-operation for the protection of personal data[299]

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;

---

297 SI and UK scrutiny reservation. FR and ES proposed that this provision should be included in another provision.

298 Some delegations (FR, PL, SI) referred to the proposal made by DE (for new Article 42a: 12884/13 DATAPROTECT 117 JAI 689 MI 692 DRS 149 DAPIX 103 FREMP 116 COMIX 473 CODEC 186) and the amendment voted by the European Parliament (Article 43a), which will imply discussions at a later stage.

299 PL thought (part of) Article 45 could be inserted into the preamble. NL, RO and 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. NL thought this article could be deleted. ES has made an alternative proposal, set out in 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394.

(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[300];

(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. (…)

[300] AT and FI thought this subparagraph was unclear and required clarification.

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46

Supervisory authority[301]

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 (…)[302]. For this purpose, the supervisory authorities shall co-operate with each other and the Commission in accordance with Chapter VII[303].

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.

---

301 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 t this is already sufficiently clear from the current text. DE indicated that it would require an intra-German consistency mechanism between the its various DPAs.

302 UK sought reassurance that the supervisory authority could also be given a wider remit, such as ensuring the freedom of information. DE remarked that it would require an intra-German consistency mechanism between the its various DPAs.

303 EE, HU, LU, SI and UK thought there was no reason to mention this duty of co-operation here.

[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[304]].

Article 47 [305]

Independence

1. Each supervisory authority shall act with complete[306] independence in performing the **duties**[307] and *exercising* the powers entrusted to it **in accordance with this Regulation**.

2. The member or members of each supervisory authority shall, in the performance of their duties and exercise of their powers **in accordance with this Regulation**[308], remain free from external influence, whether direct or indirect[309] and neither seek nor take instructions from anybody[310].

3. (…)[311]

4. (…)[312]

---

304 DE, NL, EE)that thought that this paragraph could be moved to the final provisions.
305 FR suggested merging articles 47 and 48.
306 EE, LU, SK and SI suggested deleting the word 'completely'.
307 GR scrutiny reservation.
308 Suggestion in order to allay concerns regarding the scope of the obligation of independence.
309 BE scrutiny reservation.
310 IE reservation: IE thought the latter part of this paragraph was worded too strongly.
311 AT, BE, DE and HU would prefer to reinstate this text. CZ, EE and SE were satisfied with the deletion.
312 COM and DE, AT reservation on deletion of paragraphs 3 and 4.

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[313].

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[314] of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control[315] which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public[316], annual budgets, which may be part of the overall state or national budget.

Article 48

General conditions for the members of the supervisory authority

1. Member States shall provide that the member or members[317] of each supervisory authority must be appointed (…) by the parliament and/or the government or the head of State of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure[318].

---

313 This paragraph was criticised for being too prescriptive (FR, NL, SE, SK) and too vague (LV, UK). IT raised the question of EU funding. AT thought the recital should refer to minimum requirements.

314 BG, 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. The question how to distinguish between members and staff was also raised in this context. IT thought EU resources could also be considered.

315 EE reservation.

316 Further to IE suggestion.

317 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.

318 Several delegations (FR, SE, SI and UK) thought that other modes of appointment should be allowed for. NL, LU and UK thought this should not be governed by the Regulation. FR (and RO) thought that a recital should clarify that "independent body" also covers courts.

2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers[319].

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement[320] in accordance with the law of the Member State concerned[321].

4. (…).

5. (…)[322].

Article 49

Rules on the establishment of the supervisory authority [323]

1. Each Member State shall provide by law for:

(a) the establishment (…) of each supervisory authority;

---

319 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.

320 UK thought dismissal for misconduct needed to be listed here as well. CZ stated that the terms resignation or compulsory retirement were unknown under CZ law.

321 COM reservation and DE scrutiny reservation on the expression "in accordance with the law of the Member States concerned". The question is whether this means that the Member States are being granted the power to define the duties further or whether the wording should be understood as meaning that only constitutional conditions or other legal framework conditions (e.g. civil service law) should be taken into account. DE also suggests that rules in the event of death or invalidity be added (see, for example, Article 42(4) of Regulation (EC) No 45/2001) and also suggests referring to a procedure for the nomination of a representative in case the member is prevented from performing his or her duties.

322 BE, CZ, EE, FR, LU, NL, NO, PT, SE, SK, UK are of the opinion that paragraphs 4 and 5 interfere too much with national law. CZ, NO, SE also see no need for paragraph 3. COM, DE and AT scrutiny reservation on deletion of paragraphs 4 and 5.

323 AT scrutiny reservation. 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.

(b) the qualifications (…) required to perform the duties of the members of the supervisory authority[324];

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

(d) the duration of the term of the member or members of each supervisory authority which shall not be[325] (…) 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[326];

(e) whether and, if so, for how many terms[327] the member or members of each supervisory authority shall be eligible for reappointment;

(f) the (…) conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions and occupations incompatible therewith during and after the term of office[328] and rules governing the cessation of employment[329];

(g) (…)[330].

---

324 IE reservation: IE thought these qualifications need not be laid down in law.

325 DE proposed adding a maximum term of 8 years; IT referred to 7 years.

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

327 IT thought a maximum term should be set.

328 This addition should cover what was previously stated in Article 48, (3) and (4).

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

330 CZ, NL, DE scrutiny reservation on deletion of this point.

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 *both during and after their term of office*.[331], 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[332]

Article 50

Professional secrecy[333]

(…)

[331] BE proposed adding an additional paragraph on the need to distinguish investigating and sanctioning powers, but this is dealt with by the general safeguard clause in Article 53(5). This is also true for the DE proposal for adding language concerning the duty to report an offence under national law and the privilege against self-incrimination.

[332] COM and AT scrutiny reservation on adding the provision on professional secrecy to Article 49, which concerns rules on the establishment of supervisory authorities.

[333] 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 suggestion by CZ (supported by EE, SE, SI and RO) to move this to Article 49 was followed. COM and DE scrutiny reservation on moving this provision to Article 49.

SECTION 2

COMPETENCE, TASKS AND POWERS

Article 51

Competence [334] [335]

1. Each supervisory authority shall (…) perform the tasks and exercise the powers conferred on it in accordance with this Regulation (….)[336] **on the territory of its own Member State.**

   Each Supervisory Authority shall be competent for processing taking place in the context of the activities of an establishment of a controller or a processor on the territory of its Member State or affecting data subjects on the territory of its Member State.

   a) (….)

   b) (…..)

   c) (….)

---

[334] COM reservation. Scrutiny reservation on the one-stop-shop mechanism by DE, DK, EE, FR, MT, NL, PT, RO and UK. Some delegations (BG, CY, DE, GR, NL and LU) supported one-stop-shop principle, but had many questions of understanding as to its practical implementation. Other delegations (BE, CZ, ES, FR, HU, IT, AT, PT, RO and SI) had a more critical attitude and entered a reservation. Several referred to the problem of proximity. 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). In this regard the issue of divergent MS case law was mentioned. 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.

[335] NL thought all jurisdiction rules should be set out in this article, covering both domestic and cross-border cases and private as well as public controllers (and processors). 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.

[336] DK, DE and EE queried whether the decisions of this DPA would also be binding on controllers outside that MS. Constitutional reservation by DK.

1a. *(...)*

1b. (…)

1c. (…)

2. (…)

2a. (…)

2b. (…)

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[337]. (…).

Article 51a

Competence of the lead supervisory authority

1. Without prejudice to Article 51 **and to the competences of supervisory authorities concerned**, where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State**,** or where the processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority for the main establishment or for the single establishment of the controller or the processor shall act as lead supervisory authority (…) in accordance with the **cooperation mechanism and the terms and** procedure foreseen in Article 54a**.**

337 FR, HU, NL, RO and UK scrutiny reservation. DE suggested adding "other matters assigned to courts for independent performance. The same shall apply insofar as judicially independent processing has been ordered, approved or declared admissible", as the derogation must apply whenever courts' work falls within the scope of their institutional independence, which is not only the case in the core area of judicial activity but also in areas where courts are assigned tasks specifically for independent performance.

1a. (…)[338]

2. (…)

2a. **Each supervisory authority shall be competent to deal with a complaint lodged in accordance with Article 73(1), or to deal with a possible infringement of this Regulation detected by or otherwise brought to its attention, including for seeking an amicable settlement of the complaint or infringement case and by exercising all the powers conferred on it pursuant to Article 53. That supervisory authority concerned shall inform the lead supervisory authority thereof. If the subject matter of the case concerns processing activities in other Member States or processing that substantially affects or is likely to substantially affect data subjects in other Member States, the cooperation mechanism and the terms and procedure foreseen in Article 54a shall apply.**

3. **(…)**

4. This article shall not apply where the processing is carried out by public authorities and bodies of a Member State **[or to private bodies acting on the basis of a legal obligation to discharge functions in the public interest].**

[338] Moved to Article 51(1a).

Article 51b

Identification of the supervisory authority competent for the main establishment

1. Any controller or processor which carries out processing of personal data in the context of the activities of an establishment in the Union and is established in more than one Member State [shall/**may**] indicate **its main establishment** to the supervisory **authority** where its main establishment is located (…). **That supervisory authority shall inform the European Data Protection Board of this indication.**

1a. When indicating its main establishment pursuant to paragraph 1, the controller or processor shall list all its establishments in the Union for which the decisions on the purposes and means of processing are taken at the main establishment and shall, on the request of **the** supervisory authority **concerned**, provide further information in relation to the existence of the main establishment in the place specified. The controller or processor shall inform the supervisory **authority** on any changes of the information provided.

1b. **Where necessary, t**he supervisory authority of the main establishment indicated as per paragraph 1 shall verify the existence of the main establishment at the place specified and notify the outcome of its verification to the controller or processor, the other supervisory authorities concerned and the European Data Protection Board.

2. Where there are conflicting views between the supervisory authorities concerned on which supervisory authority is (….) that for the main establishment, any of the supervisory authorities concerned may refer the matter to the European Data Protection Board. The European Data Protection Board shall **settle the dispute** on the identification of the supervisory authority for the main establishment in accordance with the procedure provided for in Article 58a.

[Article 51c

One-stop shop register[339]

The European Data Protection Board shall keep a public register of the verified information referred to in paragraph **(…).** 1a of Article 51b for consultation, which shall be electronically accessible to anyone free of charge.]

Article 52

Tasks [340]

1. Without prejudice to other tasks set out under this Regulation[341], each supervisory authority shall on its territory[342]:

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

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

(ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data[343];

---

339 ES remarked that this would be very costly.

340 DE, IT, AT, PT and SE scrutiny reservation. UK thinks the term 'functions' rather than 'duties' should be used.

341 New text as paragraphs (f) to (i) have been deleted as these duties were already laid down elsewhere in the Regulation.

342 A recital should be drafted in order to clarify that Member States may allocate other tasks to DPAs. DE thought it preferable to use the words 'at least' in the chapeau. See also new point (g) in paragraph 1.

343 NL reservation.

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

(ad) 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;

(b) deal with complaints[344] lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73[345], 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[346] , in particular if further investigation or coordination with another supervisory authority is necessary;

(c) cooperate with, including sharing information, 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 (…), including on the basis of ~~a~~ information received from 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;

---

344 IT scrutiny reservation on the term complaint; UK thought the emphasis should be on complaint-resolution.

345 BE suggested limiting this to the data subject itself.

346 IT suggested fixing a 10-weeks period for dealing with the complaint.

(f) adopt standard contractual clauses referred to in Article 26(2c);

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

(g) give advice on the processing operations referred to in Article 34(3) **(…)**[347] ;

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

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

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

(gd) (…);

(h) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;

(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;

(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;

(k) fulfil any other tasks related to the protection of personal data.

2. (…).

3. (…).

[347] Deleted as it is already in Article 53(1c)(ab).

4. Each supervisory authority shall facilitate the submission of complaints referred to in point (b) of paragraph 1, by measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

5. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer, **if any**.

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request[348]. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[349].

[348] EE pointed out that under its constitution this required an act of parliament. NL and RO also thought this should be left to Member States.

[349] DE, NL and SE reservation: this could be left to general rules.

Article 53

Powers[350] [351]

1. Each Member State shall provide by law that its supervisory authority shall have at least[352] the following investigative powers:

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

(aa) to carry out investigations in the form of data protection audits[353];

[350] DE, NL, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, RO and UK) or opposed (DE, DK, and IE) to categorising the DPA powers according to their nature. DK has raised serious constitutional concerns -based on the understanding that a decision by a "lead authority" in one Member State would be directly binding for the concerned establishments in all Member States. There is no problem if there were to be no doubt that a decision by the "lead authority" should be directed towards the "main establishment" and should *only* be binding for this establishment. It would then be for the "main establishment" – e.g. through internal business/cooperation rules – to implement the decision in subsidiaries in other Member States. If it is the case that a decision by a "lead authority" in another Member State is not to be binding for e.g. an establishment in Denmark, Denmark will not have a constitutional problem with the one-stop-shop principle. In this case the principle would not entail the transfer of powers from Danish authorities to authorities in other Member States.

[351] Several Member States (DE, FR, ~~SI~~) stated that it was unacceptable that the supervisory authority would be able to exercise these powers vis-à-vis public authorities. DE thought a distinction should 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.

[352] Further to BG suggestion, supported by EE, IT, 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. COM and ES scrutiny reservation on 'at least' in paragraphs 1 and 1a.

[353] CZ, IT, PL and SK scrutiny reservation. CZ and PL pleaded for a recital explaining that audit could be understood as inspection.

(ab) to carry out a review on certifications issued pursuant to Article 39(4);

(b) (…)

(c) (…)

(d) to notify the controller or the processor of an alleged infringement of this Regulation[354] (…);

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

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

1a. (…).

1b. Each Member State shall provide by law that its supervisory authority shall have the following corrective powers:

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

(b) to issue reprimands[355] to a controller or processor where processing operations have infringed provisions of this Regulation[356];

(c) (…);

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

---

354 BE suggested adding the power to oblige the controller to communicate the personal data breach to the data subject.

355 PL and SK scrutiny reservation.

356 PL scrutiny reservation on points (a) and (b).

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; in particular by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17 and 17a and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;

(e) to impose a temporary or definitive limitation on processing;

(f) to order the suspension of data flows to a recipient in a third country or to an international organisation[357];

(g) to impose an administrative fine pursuant to Articles 79 and 79a, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.

1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 34[358],

(aa) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, (…) in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(ab) to authorise processing referred to in Article 34(7a);

(ac) to issue an opinion and adopt draft codes of conduct pursuant to Article 38(2);

(ad) to accredit certification bodies under the terms of Article 39a;

---

357 SK reservation.

358 NL scrutiny reservation. This was placed in the wrong category.

(ae) to issue certifications in accordance with Article 39(2a);

(b) authorise standard data protection clauses referred to in point (c) of Article 42(2);

(c) authorise contractual clauses referred to in point (d) of Article 42(2);

(d) approve binding corporate rules pursuant to Article 43.

2. *The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.*[359]

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(…), where appropriate, to commence or engage otherwise in legal proceedings[360], in order to enforce the provisions of this Regulation[361].

4. (…)

5. (…)

Article 54

Activity Report

Each supervisory authority shall draw up an annual report of its activities. The report shall be transmitted to the national Parliament, the government and other authorities as designated by national law. It shall be made available to the public, the European Commission and the European Data Protection Board.

---

359 CY, ES, FR, IT and RO thought this could be put in a recital as these obligations were binding upon the Member States at any rate. COM could accept this.

360 DE, FR and RO reservation on proposed DPA power to engage in legal proceedings. UK scrutiny reservation. CZ reservation on the power to bring this to the attention of the judicial authorities.

361 DE thought para. 3 and 4 should be deleted.

CHAPTER VII[362]

CO-OPERATION AND CONSISTENCY

SECTION 1

CO-OPERATION

Article 54a

Cooperation between the lead supervisory authority and other supervisory authorities concerned[363]

1. In the cases referred to in (…) Article 51a, (….) the lead supervisory authority (…) shall cooperate with the supervisory authorities concerned in accordance with this article **(…)** in an endeavour to reach consensus (…). (…)

1a. In the cases referred to in paragraph 1 of Article 51a, each supervisory authority concerned shall inform the lead supervisory authority and refer the matter to the lead supervisory authority **without delay (…).**

2. (…) The lead supervisory authority shall, without delay, further investigate the subject matter and communicate the relevant information on the matter to the supervisory authorities concerned and shall **(…)** submit a draft decision **including** on **whether there is an infringement of this Regulation or not and on the exercise of the powers referred to in paragraphs 1, 1b and 1c of Article 53** (…) to all supervisory authorities concerned for their opinion and take due account of the views of those supervisory authorities.

---

362 AT and FR scrutiny reservation on Chapter VII.

363 BE, CZ, CY, DE, EE, FR, FI, IE, LU, RO, PT and NL scrutiny reservation. IE pointed out that in the case of personal data processed by social media or other internet platforms, all 28 MS DPAs would be 'concerned'. LU and NL doubted that one DPA concerned would be sufficient to trigger the consistency mechanisms. BE, FR, PL and LU expressed a preference for amicable settlements.

a) (…)

b) (…)

c) (…)

2a. (…)

2b. The lead supervisory authority may request at any time **the** supervisory authorities **concerned** to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. Where any of the supervisory authorities concerned expresses a reasoned objection within a period of four weeks after having been consulted in accordance with paragraph 2 to the draft decision, the lead supervisory authority shall, if it does not follow the objection, submit the matter to the consistency mechanism referred to in Article 57. In such a case, the (…) European Data Protection Board shall settle the **dispute** and be binding on the lead supervisory authority and all the supervisory authorities concerned pursuant to point 2(a) of Article 57 and Article 58a. Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft decision.

4. Where no supervisory authority concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraph 3, the lead supervisory authority and the supervisory authorities concerned shall agree on a single decision jointly.

4a. The lead supervisory authority shall **give legal effect to the jointly agreed single decision** and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and inform the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds.

4b. Where (…) the jointly agreed **single decision** concerns a complaint and as far as it adversely affects the complainant, notably where the complaint is rejected, dismissed or granted only in part, (…) **the** supervisory authority that **has** received such complaint shall **give legal effect to the jointly agreed** the single decision concerning that complaint and serve it on the complainant. The complainant shall be informed in any case of the outcome of the complaint pursuant to Article 73, paragraph 5.[364]

4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall then inform all the supervisory authorities concerned. The supervisory authorities concerned shall be bound by the single decision adopted jointly in the manner described above.

4d. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.

5. The lead supervisory authority and the supervisory authorities concerned shall supply the information required under this Article **(…)** to each other by electronic means, using a standardised format.

---

364 PL scrutiny reservation on paragraph 4b.

Article 54b

Cooperation between the lead supervisory authority and the other supervisory authorities concerned in individual cases of possible non-compliance with the Regulation

(…)

Article 55

Mutual assistance[365]

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. (...)

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[366] after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation (…).

3. The request for assistance shall contain all the necessary information[367], 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.

---

365 DE, NL SE and UK scrutiny reservation. Several other delegations indicated that further clarity was required on this fundamental Article and the concept of mutual assistance, and announced text proposals: EE pleaded for much more detailed rules on mutual assistance, as is already the case in civil and criminal law. AT, supported by DE, declared that it had no specific problem with this Article, but that, in general, there was a need to follow developments in relation to CoE Convention No. 108.

366 ES had suggested reducing it to 15 days. PT supported the suggestion of two weeks, with a possibility of adding more time, if needed. RO, on the other hand, found one month too short, and requested SE remarked that this timeline might be unrealistic in some cases. COM indicated that it was only a deadline for replying, but that paragraph 5 allowed longer periods for executing the assistance requested. UK requested a timetable, indicating deadlines.

367 EE and SE scrutiny reservation.

4. [368]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 or for the measures it is requested to execute[369]; 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.

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[370].

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means[371], 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 authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances[372].

---

368 SE indicated further scrutiny was required as to whether other grounds of refusal were required. UK thought that this paragraph was drafted in much too absolute a fashion.

369 Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI. NL and IT asked for further clarification.

370 RO scrutiny reservation.

371 PT (supported by RO) suggested adding "or other means if for some reason, electronic means are not available, and the communication is urgent".

372 PT, UK and DE asked for clarification in relation to the resources needed / and estimate of costs.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure[373] on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57[374].

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months[375]. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board (…) 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)[376].

---

373 LU requested more clarification with regard to what would happen if this provisional measure were not confirmed.

374 EE, FR, RO, and UK reservation. DE scrutiny. UK did not find the drafting sufficiently clear, for instance regarding which authority would be competent and action on other Member States territory. COM specified that this Article would apply specifically in bilateral relations (whereas Article 56 would cover joint operations), the underlying philosophy being to avoid extraterritorial activity.

375 DE asked for deletion of this deadline; the measure should be withdrawn if the conditions for imposing it were no longer fulfilled.

376 DE, IT, EE, CZ and NL reservation. EE questioned whether implementing acts where necessary for this purpose. ES reminded about its proposal for an Article 55a.

Article 56

Joint operations of supervisory authorities[377]

1. The supervisory authorities may, where appropriate, conduct joint operations, including joint investigations and joint enforcement measures in which members or staff from other Member States' supervisory authorities are involved.

2. In cases where the controller or processor has establishments in several Member States or where [a significant number of[378]] data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations, as appropriate. The competent supervisory[379] authority shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond without delay to the request of a supervisory authority to participate[380].

---

377 IT requested a specification in this Article that this was also about multilateral cooperation. FR asked for a clearer distinction between Articles 55 and 56. DE, EE, PT and UK scrutiny reservation. Several delegations (DE, LV, NL, SE, IT, UK) 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. LU indicated it was not convinced of the added value of joint investigations. UK requested to make sure that these mechanisms would work in practice and drew the attention to the fact that paragraphs 1 and 3 were discretionary, whereas paragraph 2 was binding, and that this was confusing and potentially contradictory.

378 COM reservation; more criteria should be added IT, supported by FR, BE and CZ suggested stressing the multilateral aspect by adding text.

379 LU asked for a clarification of who would be the lead authority. UK stated that it seemed like a mix of Art. 51(1) and 51(2) competences.

380 SE entered a favourable scrutiny reservation on this paragraph.

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 law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…) [381]

3a. Where, in accordance with paragraph 1, staff of a seconding supervisory authority are operating in another Member State, the Member State of the host supervisory authority shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the (…) persons entitled on their behalf.

3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages [it has sustained] from another Member State[382].

4. (…)

---

381 DE, LU, PT and COM scrutiny reservation on the deletion of this last phrase.

382 Inspired by Article 3 of the Council Framework Decision of 13 June 2002 on joint investigation teams. UK reservation on paras. 3a, 3b and 3c.

5. [383]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[384]

Article 57

Consistency mechanism[385]

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[386].

1a. (…)

1b. (…)

---

383 NL asked whether the measures of paragraphs 5 and 6 were really necessary. EE suggested a merger of the two paragraphs.

384 BE, IT, SK and SI scrutiny reservation. BE reservation on the time required for a consistency mechanism procedure. DE parliamentary reservation and BE and UK reservation on the role of COM in the consistency mechanism.

385 EE, FI, LU, NL and UK scrutiny reservation.

386 CZ, DE, ES and RO 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.

2. The European Data Protection Board shall **(…)** issue an opinion whenever a competent *supervisory authority* intends *to adopt* any of the measures below (…). To that end, the competent supervisory authority shall communicate the draft measure to the European Data Protection Board, when the measure:

(a) (…);

(b) (…);

(c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assessment 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 accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph **2a of Article 39 or paragraph** 3 of Article 39a;

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

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

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

2a. The European Data Protection Board shall **settle a dispute between supervisory authorities** in the following cases:

a) Where, in a case referred to in paragraph 3 of Article 54a(…), a supervisory authority concerned (…) expresses a reasoned objection to a draft measure **notably whether there is an infringement of this Regulation or not**. In that case, the lead supervisory authority shall communicate the matter to the European Data Protection Board in order for the Board to definitively settle the conflicting views on the draft measure;

b) Where, in a case referred to in paragraph 2 of Article 51b, there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment. In that case, any of the supervisory authorities concerned may communicate the matter to the European Data Protection Board (…);

c) Where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56. In that case, any supervisory authority concerned[387], the lead supervisory authority or the Commission may communicate such matter to the European Data Protection Board[388];

[387] BE, IT, SE, SI, SK and PL thought the scope of this paragraph should be limited so as to limit the number of cases.

[388] 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.

d) Where a competent supervisory authority does not request the opinion of the European Data Protection Board in the cases mentioned in paragraph 2 of this Article, or does not intend to follow the opinion of the European Data Protection Board issued as per Article 58. In that case, any supervisory authority concerned, the lead supervisory authority or the Commission may communicate the matter to the European Data Protection Board.

2b. The lead supervisory authority shall inform the European Data Protection Board within three weeks of any measure adopted pursuant to Article 54a(4a) and also provide a summary of the facts and grounds that made the taking of such measure necessary.

2c. Any supervisory authority (…), the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion.

4. (…)

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

6. The chair of the European Data Protection Board shall without undue delay electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the European Data Protection Board shall, where necessary, provide translations of relevant information.

Article 58

Opinion by the European Data Protection Board[389]

1. (…)

2. (…)

3. (…)

4. (…)

5. (…)

6. (…)

7. In the cases referred to in paragraphs 2 and 2c of Article 57, the European Data Protection Board shall issue an opinion on the subject- matter submitted to it provided it has not already issued an opinion on the same matter[390]. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. This period may be extended by a further month, taking into account the complexity of the subject matter. [Regarding the draft decision circulated to the members of the Board in accordance with paragraph 6 of Article 57, a member which has not objected within the period indicated by the Chair, shall be deemed to be in agreement with the draft decision.]

389 NL and UK scrutiny reservation.

390 ES suggested keeping the possibility for one DPA requesting an opinion from the EDPB.

7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft measure as per paragraph 2 of Article 57.

7b. 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 2c 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 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 will amend its draft measure and, if any, the amended draft measure, using a standardised format.

9. Where the supervisory authority concerned informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph 2a of Article 57 shall apply.

10. (…)

11. (…)

Article 58a

Dispute Resolution by the European Data Protection Board

1. In the cases referred to in paragraph 2a of Article 57, the European Data Protection Board shall **settle the dispute** on the subject-matter submitted to it in order to ensure the correct application of this Regulation in individual cases.

2. The **European Data Protection Board shall take its position on the dispute** referred to in paragraph 1 (…) within one month from the referral of the subject-matter by a two-third majority of **its** members. The absence of any response shall not be deemed to signify agreement (…). This period may be extended by a further month on account of the complexity of the subject-matter.

3. The supervisory authorities concerned and the lead authority, as the case may be, may not adopt a decision on the subject-matter submitted to the Board under paragraph 1 during the period referred to in paragraph 2.

4. The **position on the dispute** referred to in paragraph 1 shall state the underlying reasons.

5. The **position on the dispute** referred to in paragraph 1 shall be binding (…) and addressed **to** the supervisory authorities concerned and the lead authority, as the case may be.

6. The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned and the lead authority **(…)** [391]. It shall inform the Commission thereof.

7. The supervisory authorities concerned shall, on the basis of the **settlement of the dispute** referred to in paragraph 1, **notably whether there is an infringement of this Regulation or not,** without undue delay and at the latest by one month after service of such **position on the dispute**, adopt their final decision on the **case** under the terms of Article 54, paragraph**s** 4a **and 4b**.

[391] IE asked whether the Chair would notify this directly to the complainant.

Article 59

Opinion by the Commission[392]

(…)

Article 60

Suspension of a draft measure[393]

(…)

Article 61

Urgency procedure[394]

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 or the procedure referred to in Article 54a, immediately adopt provisional measures intended to produce legal effects (…) for the territory of its own Member State[395], 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[396].

---

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

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

394 DE scrutiny reservation. 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.

395 COM scrutiny reservation.

396 The conditions under which the EDPB needed to be informed also gave rise to questions (ES). COM stated the obligation only existed in cross-border one-stop-shop mechanism cases.

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 or an urgent binding **settlement of the dispute** from the European Data Protection Board, giving reasons for requesting such opinion or **settlement of the dispute**.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the European Data Protection Board 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 or **settlement of the dispute**, including for the urgent need to act.

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

Article 62

Implementing acts

1. The Commission may adopt implementing acts of general scope for:

(a) (…)[397]

(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(5) and (6) and in Article 58(8).

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

[397] COM reservation on deletion.

2. (…)

3. (…)

Article 63

Implementation of measures adopted by way of the consistency mechanism[398]

(…)

[398] Deleted further to EE and SI reservation and DE and DK scrutiny reservation.

SECTION 3

EUROPEAN DATA PROTECTION BOARD[399]

Article 64

European Data Protection Board[400]

1a. The European Data Protection Board is **hereby** established as body of the Union and shall have legal personality.

1b. The European Data Protection Board shall be represented by its Chair**.**

2. The European Data Protection Board shall be composed of the head[401] of one supervisory authority of each Member State or his/her representative and of the European Data Protection Supervisor[402].

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[403] shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative without voting rights. The chair of the European Data Protection Board shall, communicate the Commission the activities of the European Data Protection Board.

---

399 Several Member States (BE, DE, HR, IT, PL and 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.

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

401 BE, supported by CZ, CY, SE and SI, suggested adding "*or his/her representative"*. IT suggested referring to Art. 68(2).

402 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.

403 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 or exercising its powers pursuant to Articles 66 (…) and 67.[404]

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 or the exercise of its powers, neither seek nor take instructions from anybody[405].

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:

   (aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(2a) without prejudice to the tasks of national supervisory authorities;

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

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

   (ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a[406];

---

404 UK and SI scrutiny reservation.

405 DE scrutiny reservation.

406 DK reservation on the introduction of administrative fines in the text and meant that it was for national authorities to decide on that.

(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;

(caa) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4 of Article 39[407];

(cab) specify the requirements mentioned in paragraph 3 of Article 39a with a view to the accreditation of certification bodies under Article 39;

(cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to in Article 41;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in paragraph 2 and **on matters submitted pursuant to paragraph** 2c of 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;

[(h) maintain a publicly accessible electronic register for consultation on confirmed main establishments referred to in Article 51c;]

(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues dealt with in the consistency mechanism.

---

407 HU said that paragraphs (caa) and (cab) were contrary to the text of the general approach reached in June 2014 (11028/14); it is for the national supervisory authority to do this.

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, 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.

Article 67

Reports

1. (…)

2 The European Data Protection Board *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) as well as of the **settlement of the disputes** referred to in paragraph **(…) 2a** of Article (…) **57**.

Article 68

Procedure

1. The European Data Protection Board shall[408] **settle disputes** referred to in paragraph **2a** of Article **57** by a two-third majority of its members**.** As regards decisions related to the tasks listed in Article 66 hereof, they shall be taken by a simple majority of its members (…).

2. The European Data Protection Board shall adopt its own rules of procedure **by a two-third majority of its members** and organise its own operational arrangements[409].

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members (…).[410]

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable once[411].

---

408 Some delegations suggested replacing this term that could give rise to confusion, with another, such as for instance "resolution". COM would consider an alternative.

409 CZ asked with what majority the rules of procedure would be taken.

410 COM found this problematic and maintained its reservation on deletion.

411 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 and SK scrutiny reservation.

Article 70

Tasks of the chair

1. The chair shall have the following tasks[412]:

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

   (aa) to notify **positions of** the European Data Protection Board **on the settlement of disputes pursuant to Article 58a** to **the lead supervisory authority and** the supervisory authorities concerned (…);

   (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[413].

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

---

412 BE suggesting adding another task, namely the chair's role towards the exterior.

413 DE, EE, FR, ES, **HU, AT, IRL,** RO, PT, SI, SK and UK reservation on entrusting the EDPS with the EDPB secretariat. The risk of conflicts of interest of EDPS staff was also raised. FR and UK inquired about the costs. NL scrutiny reservation.

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, **positions on the settlement of disputes between supervisory authorities** and other texts adopted by the European Data Protection Board.

Article 72

Confidentiality[414]

1. The discussions[415] 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.

---

414 DE, EE, ES, RO, PL, PT, 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. This article should be revisited once there is more clarity on the exact role and powers of the board, including the question whether the EDPS shall ensure the Secretariat.

415 IT scrutiny reservation: it suggested replacing this term with 'minutes' or 'summary records', thereby distinguishing between confidentiality of decision-making and access to documents.

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS[416]

Article 73

Right to lodge a complaint with a supervisory authority[417]

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[418] in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation[419].

2. (…)

3. (…)

4. (…)

5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant Article 74[420] or, as regards decisions taken by the European Data Protection Board pursuant to Article 76b.

---

416 AT, FR, EE, ES and RO scrutiny reservation.

417 BE, CY, CZ, EE, IE, LY, PT and SI scrutiny reservation.

418 COM, BG, IT and LU though that the data subject should be able to lodge a complaint with any DPA without limitation since the protection of personal data was a fundamental right.

419 DE, supported by NL, suggested adding "when its rights are not being respected".

420 NL and FR scrutiny reservation. Article 54c (2) already provides for a general duty for the supervisory authority with which a complaint has been lodged to notify the data subject of any measures taken (i.e. the scenario of a 'positive' reply by the DPA).

Article 74

Right to a judicial remedy against a supervisory authority[421]

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 legally binding decision of a supervisory authority concerning them. (...)[422].

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority competent in accordance with Article 51[423] does not deal with a complaint or does not inform the data subject within three months or any shorter period provided under Union or Member State law[424] on the progress or outcome of the complaint lodged under Article 73[425].

3. Proceedings against a (…) supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established[426].

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

4. (…)

5. (…)[427]

---

421 ES, PT and SI reservation. EE, IT and UK scrutiny reservation.

422 DE, supported by IE and SE, suggested adding: 'by which it is adversely affected'.

423 COM reservation.

424 SI indicated that under its law the DPA was obliged to reply within two months.

425 SE scrutiny reservation. BE reservation. BE said that there was a link to Article 53 and the main establishment and the DPA of the habitual residence. Support from NL. IT thought that paragraphs 1 and 2 overlapped. NO wanted to delete paragraph 2 since a court review would endanger the independency of the DPA.

426 IT suggests stating that proceedings may be brought before the courts of the Member state where the natural or legal person has his/her habitual residence or is established.

427 COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.

Article 75

Right to a judicial remedy against a controller or processor[428]

1. Without prejudice to any available administrative or non-judicial remedy[429], 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[430] if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment (…)[431]. 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 or processor is a public authority acting in the exercise of its public powers.

3. (…)

4. (…)

---

428 DE, EE, PL, PT, SI and SK scrutiny reservation. ES, IT reservation.

429 SI wanted to delete *non-judicial remedy*.

430 ES asked how judicial remedy would be interpreted and how a missed deadline or that there will be no judicial review would be considered.

431 In view of the concerns raised, the reference to national law has been kept only in recital 113.

Article 76 [432]

Representation of data subjects

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 statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data,*[433] *to lodge the complaint on his or her behalf* [434] and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf[435].

1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1[436] shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51[437] 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.[438]].

---

432 DE, ES, PT, RO and SI scrutiny reservation. CZ, EE, IT, NL, SI and UK thought this article was superfluous.

433 COM said that consumer organisations and data protection organisations enhance fundamental rights so it was important that they could lodge complaints.

434 IT scrutiny reservation.

435 DE parliamentary reservation; BE, EE reservation and IT scrutiny reservation. EE, supported by FI and SE, thought that the data subject could choose anybody to represent her/him so this drafting was a limitation so a reference to national law was needed. Support from SE.

436 PL asked how an organisation could know about a breach. PT did not want to exclude the possibility of an organisation to lodge complaint if that was provided in national law but meant that the wording was not clear.

437 COM reservation on limitation to competent supervisory authority.

438 This paragraph was moved from Article 73(3). BE, EE, FR reservation. BG, DE, DK, IT, LU, NL, PT and UK scrutiny reservation. UK in particularly queried whether such possibility would also be open to an association when the data subject itself considered that the reply he/she had received was satisfactory. ES on the contrary thought that this possibility should not be limited to data breaches. UK thought that paragraph 1 was sufficient. For DK, PL and SE it was not acceptable that an organisation etc. had an independent right to lodge a complaint.

2. (…)

3. (…)

4. (…)

5. (…)[439]

Article 76a

Suspension of proceedings[440]

1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are pending in a court in another Member State, it shall[441] contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings involving the same processing activities are pending in a court in another Member State, any competent court other than the court first seized may suspend[442] its proceedings.

---

439 COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.

440 AT, BE, DK, EE, ES, FI, FR, IT, NL, PL, PT, SE and SI scrutiny reservation. ES thought that *lis pendens* necessitated the same persons, same proceeding, same object of dispute and same claim and that that could be difficult to establish.UK, supported by FR, cautioned against having a too prescriptive text, support from FR SE thought that GDPR should not regulate *lis pendens*, instead it should be up to the DPA and MS courts to decide. For LU this was a question of judicial cooperation between judicial authorities. NO and FR asked how this text related to Regulation No 44/2001 and the Lugano Convention FI considered that it was necessary to have rules on this question in GDPR.

441 LU supported by EL, suggested to replace "shall" with "may".

442 NL and PL thought that it was difficult to force courts to stay proceedings waiting for another court to decide. NL asked how it was possible for a court to know that another case was going on elsewhere. COM thought that limitation to "same parties" was not appropriate here.

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.[443]

Article 76b

Actions before the Court of Justice of the European Union against decisions by the European Data Protection Board

1. Actions may be brought before the Court of Justice of the European Union in accordance with Article 263 TFEU, in order for it to review the legality of decisions taken by the European Data Protection Board pursuant to Article 58a. Such actions may be brought before the Court of Justice of the European Union by supervisory authorities, Member States and the Union institutions as well as by natural or legal persons to whom decisions taken by the European Data Protection Board have been notified or to whom such decisions are of direct and individual concern, including data subjects who have lodged a complaint in accordance with Article 73.

2. The expiration of the time-period provided for in the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court shall not bar the persons referred to in paragraph 1 from calling in question the lawfulness of any decision taken by the European Data Protection Board before the national courts in accordance with Article 74 or 75 and those national courts from requesting the Court of Justice of the European Union a preliminary ruling concerning the validity of any decision taken by the European Data Protection Board in accordance with Article 267 TFEU

[443] Based on Article 28 of Brussels I Regulation.

3. Where the European Data Protection Board notifies its decision in accordance with Article 58a(6), such a notification shall state the possibility for the persons referred to in paragraph 1 to bring an action for annulment before the General Court of the European Union in accordance with Article 263 TFEU as well as the time-period for such an action in accordance with the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court. It shall also refer to the additional right conferred on that person pursuant to paragraph 2.

4. In the event that the European Data Protection Board has an obligation to act and fails to take a decision, proceedings for failure to act may be brought before the Court of Justice of the European Union in accordance with Article 265 TFEU.

5. The European Data Protection Board shall be required to take the necessary measures to comply with the judgment of the Court of Justice of the European Union.

Article 77

Right to compensation and liability[444]

1. Any person who has suffered [445]damage[446] as a result of a processing operation which is not in compliance [447] with this Regulation shall have the right to receive compensation from the controller or processor[448] for the damage suffered.[449]

2. [450]Where more than one controller or processor or a controller and processor are involved in the processing which gives rise to the damage, each controller or processor shall be jointly[451] and severally liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors[452].

---

444 Several Member States (DE, NL and UK) have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. IT suggested specifying that these rules are to be applied according to national law, support from CZ, NL, RO and SI. COM thinks that it has to be left to ECJ to interpret these rules and concepts. FR scrutiny reservation; FR questioned the division of responsibilities and the link to Articles 24 and 25 and national law in this field as well as the principle of subsidiarity.

445 DE, HU and SK suggested adding "material or immaterial/moral". NO suggested clarifying this in a recital.

446 BE asked whether a violation of the principles of the Regulation was enough to constitute a damage or whether the data subject had to prove a specific damage (*obligation de moyens ou de résultat*). COM said that the data subject had to prove the damage.

447 COM reservation as the current draft (contrary to the initial version and the 195 Directive) no longer embodies the principle of strict liability.

448 DE suggested restricting the possibility to seek compensation from the processor to cases where, in violation of point (a) of paragraph 2 of Article 26, the processor has processed personal data contrary to or in the absence of instructions from the controller. ES suggested adding a reference to 'a right to exercise a direction action', but this is already encompassed in the current draft.

449 SE supported by HU considered that Article 77 was unclear and wanted to know whether both an economic and immaterial damage was covered.

450 IE queried why the reference to Article 24(2) had been removed and then the second sentence had been added: what the purpose to bring a claim against all of them and then sort out the individual responsibility?

451 UK thought that one controller or processor might be more responsible than another so it should be allowed for a relative responsibility. SE said that according Directive 95/46 (Article 23) the burden of proof and division of responsibility between the controller and the processor it was only the controller that was held responsible.

452 SI reservation: SI thought this paragraph could be deleted and left entirely to national law.

3. The controller or the processor may[453] 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[454].

4. Court proceedings for exercising the right to receive compensation shall be brought before the courts with jurisdiction for compensation claims under national law of the Member State referred to in paragraph 2 of Article 75.

Article 78

Penalties

(…)[455]

[453] PL thought this should be turned into a mandatory provision.

[454] DE and PL thought this paragraph needed to be further elaborated. DE in particular thought that the relationship to Article 39 needed to be further clarified. SI thought an arrangement for strict liability in the case of processing by public bodies should be inserted into this paragraph.

[455] This Article was moved to Article 79b. Scrutiny reservation by SK, RO and PT.

Article 79

General conditions for imposing administrative fines[456]

1. Each supervisory authority [competent in accordance with Article 51] shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 53[457].

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

2a. When deciding whether to impose an administrative fine in addition to, or instead of, measures referred to in points (a) to (f) of paragraph 1b of Article 53[458] and [459]deciding on the amount of the administrative fine in each individual case due regard shall be had to the following:

(a) the nature, gravity and duration of the infringement 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;

---

456 DK reservation: it indicated that this system of administrative fining was incompatible with its constitutional legal system. PL thought that Article 79 should set out guidelines only, with possibly a maximum threshold for the DPA to impose fines.

457 Some delegations thought that the corrective measures of Article 53 (1b) should be listed rather here.

458 Moved here from paragraph 2b (further to remarks by FR, IE, IT and CZ).

459 Some delegations (EE, SK, PL) thought that aggravating circumstances should be distinguished from mitigating circumstances. SK suggested laying down exact thresholds (e.g. more than 2/3 of the maximum fine in case of aggravating circumstances). IT thought the possibility of EDPB guidance should be referred to here. NL thought that the status of codes of conduct and certification as well as the consequences of adhering to them needed to be looked at.

(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 pursuant to Articles 23 and 30;

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

[(g) any financial benefits gained, or losses avoided, directly or indirectly from the infringement[460];]

(h) the manner 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[461];

(i) **in case** measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, **have previously been** ordered against the controller or processor concerned with regard to the same subject-matter[462], *compliance with **these measures*** ;

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39[463];

---

460 DK, ES and SI reservation. SI stated that a DPA was not equipped to assess this.

461 CZ was concerned that this factor might amount to a violation of the privilege against self-incrimination

462 This should also accommodate concerns regarding the privilege against self-incrimination by removing a general reference to co-operation in the investigation. IT thought this paragraph should refer more generally to previous incidents. DE pleaded for its deletion.

463 DE reservation: DE pointed out that non-adherence to approved codes of conduct or approved certification mechanisms could as such not amount to a violation of the Regulation.

(k) (…)[464];

(l) (…)[465];

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

2b. (…).

3. (…)[466]

3a. (…)[467]

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[468].

4. The *exercise by the supervisory authority* [competent in accordance with Article 51] 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.

---

464 Removed at the suggestion of DE and SK.

465 If Member states are entirely free to decide whether or not to provide for sanctions against public authorities, it does not seem appropriate to list the fact that the controller is a public body here.

466 COM reservation on deletion; linked to reservation on Article 79a.

467 COM reservation on deletion.

468 DE would prefer to rule out this possibility in the Regulation. ES thought it should be provided that no administrative fines can be imposed on the public sector.

Article 79a

Administrative fines[469][470]

1. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] %[471] of its total worldwide annual turnover[472] of the preceding financial year, on a controller who, intentionally or negligently[473]:

(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 the first sentence of paragraph 4 of Article 12.

---

469 DE, EE, ES, PT and SI scrutiny reservation. FI and SI reservation. COM reservation on replacing 'shall' by 'may' and the deletion of amounts and percentages in paragraphs 1, 2 and 3. DE wanted the risk-based approach to be made clearer. DE thought that proportionality was important because Article 79a concerned fundamental rights/rule of law and deemed it disproportionate that a supervisory authority could impose a fine that the data subject was unaware of. DE said that it was necessary to set out the fines clearly and that the one-stop shop principle did not allow for exceptions being set out in national law. IE thought e gravity of offences was not sufficiently illustrated, *e.g.* infringement in para. 3(m), which according to IE is the most serious one. FR reservation: the strictness of the text may impinge on the independence of the DPA.

470 A majority of Member States (BE, CY DE, EE, ES, FI, IT, LV, LU, MT and NL) appear to be in favour of different scales of sanctions. COM referred to the Market Abuse Regulation with three levels of fines. DK, HU, IE, SE and UK were opposed to maintaining different sanctions scales. FR and PL did not favour it, but could accept it.

471 EE did not consider it appropriate to set out sanctions in percentage because the sanction was not predictable.. PT considered that there should be minimum penalties for a natural person and that for SMEs and micro enterprises the volume of the business should not be looked at when applying the fines (this factor should only be applicable for multinationals). PL thought that administrative fines should be implemented in the same way in all MS. PL said that the fines should be flexible and high enough to represent a deterrent, also for overseas companies

472 UK commented that *turnover* was used in competition law and asked whether the harm was the same here. EE asked how the annual turnover was connected to the sanction. SI thought that compared to competition law where the damage concerned the society as a whole, data protection concerned private infringements. COM said that both competition law and data protection concern economic values, whereas data protection protects values of the data subject.

473 IT wanted to delete "intentionally or negligently" and thought that those notions were already integrated part of the mechanism to calculate fines.

2. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual (…) turnover of the preceding financial year[474], on a controller or processor who, intentionally or negligently:[475]

(a) does not provide the information, or (…) provides incomplete information, or does not provide the information timely or in a sufficiently transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;

(b) 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;

(c) (…);

(d) (…);

(e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;

(f) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4).

(g) (…)

[474] DE suggestion.

[475] IT considered that paragraphs 2 and 3 were very generic and only described the infringements but that the scale of gravity was not well defined. IT asked for a better categorisation of the infringements.

3. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year[476], on a controller or processor who, intentionally or negligently:

(a) processes personal data without a (…)[477] 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);

(j) (…);

(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;

---

476 DE suggestion.

477 FI pointed out that "sufficient" was unclear taking into consideration of the principles in Article 6 (f).

(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) (…)[478]

(o) (…).

[3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.]

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.][479]

[478] IT wanted to reinstate failure to cooperate with the DPO. IE that thought that this was a subjective infringement.

[479] CZ, DE, NL and RO reservation. NL that thought that guidelines from the EDPB could solve the problems on the amounts. CZ wanted to delete the paragraph and thought that the DPA could set out the amounts.

Article 79b

Penalties[480]

1. *For infringements of the provisions of this Regulation not listed in Article 79a Member States shall*[481] *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*.

---

480 DE, DK, EE, ES, IT, PL and PT and SK scrutiny reservation. COM explained that infringements not listed in Article 79a were those under national law, referred to in Chapter IX, for example infringements in employment law and relating to freedom of expression. In that way Article 79b is complementary to the list in Article 79and does not exclude other penalties. IT thought it was better to delete the Article but lay down the possibility to legislate at national level. FR reservation on the imposition of criminal penalties. DE in favour of referring *expressis verbis* to criminal penalties.

481 BE and EE reservation.

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80

Processing of personal data and freedom of expression and information

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

2. For *the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression*, Member States shall[482] provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency)[483] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (…).

---

[482] HU, AT, SI and SE reservation; they would prefer not to limit this paragraph to journalistic processing.

[483] BE, DE, FR, IE and SE had requested to include also a reference to Chapter VIII. This was opposed to by COM. The Presidency points out that in case the freedom of expression prevails over the right to data protection, there will obviously no infringement to sanction. Where an infringement is found to have place, the interference with the freedom of expression will have to taken into account as an element in the determination of the sanction. This application of the proportionality principle should be reflected in Chapter VIII.

Article 80a

Processing of personal data and public access to official documents [484]

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest 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 official documents with the right to the protection of personal data pursuant to this Regulation.

Article 80aa

Processing of personal data and reuse of public sector information

Personal data in in public sector information held by a public authority or a public body or a private *body* for the performance of a task carried out in the public interest *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 the reuse of such official documents and public sector information with *the right to the protection of personal data pursuant to this Regulation*[485].

[484] SK and PT scrutiny reservation.

[485] COM reservation in view of incompatibility with existing EU law, in particular Directive 2003/98/EC (as amended by Directive 2013/37/EU).

Article 80b [486]

Processing of national identification number

Member States may determine the specific conditions for the processing of a national identification number or any other identifier of general application. In this case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 81

Processing of personal data for health -related purposes

(…)[487]

Article 81a

Processing of genetic data

(…)[488]

[486] DK, PL, SK scrutiny reservation.

[487] See Article 9(2)(g),(h), (hb) and (4) which enshrine the basic idea, previously expressed in Article 81, that sensitive data may be processed for purposes of medicine, health-care, public health and other public interests, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

[488] See Article 9(2)(ha) and (4) which enshrine the basic idea, previously expressed in Article 81a, that genetic data may be processed, e.g. for medical purposes or to clarify parentage, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

Article 82

Processing in the employment context

1. Member States may by law or by collective agreements, provide for more specific[489] rules to ensure the protection of the rights and freedoms in respect of 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, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property 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. Member States may by law determine the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee[490].

Article 82a

Processing for purposes of social protection

(…)

[489] DE, supported, by AT, CZ, HU, DK and SI, wanted to refer to 'stricter' rules.

[490] This paragraph may need to be looked at again in the context of the discussions on Articles 7 and 8 for consent. COM, PL, PT scrutiny reservation.

Article 83

Derogations applying to processing of personal data for archiving, scientific, statistical and historical purposes

1. Where personal data are processed for scientific, statistical[491] or historical purposes Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19[492], insofar as such derogation is necessary for the fulfilment of the specific purposes.

1a. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 and 53 (1b)(d) and (e), insofar as such derogation is necessary for the fulfilment of these purposes[493].

1b. In case a type of processing referred to in paragraph**s** 1 and 1a serves at the same time another purpose, the derogations allowed for apply only to the processing for the purposes referred to in those paragraphs.

2. The appropriate safeguards referred to in paragraphs 1 and 1a shall be laid down in Union or Member State law and be such to ensure that technological and/or organisational protection measures pursuant to this Regulation are applied to the personal data (…), to minimise the processing of personal data in pursuance of the proportionality and necessity principles, such as *pseudonymising the data,* unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled within reasonable means.

3. (…).

---

491 PL and SI would want to restrict this to statistical processing in the public interest.

492 NL and DK proposed adding a reference to Article 7. SI supported this as far as scientific processing is concerned. PL suggested deleting the reference to Article 19.

493 COM and AT thought the list of articles from which can be derogated should be more limited.

Article 84

Obligations of secrecy [494]

1. (…) Member States may adopt specific rules to set out the (…) powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects under Union or Member State law or rules established by national competent bodies to an obligation of professional secrecy**,** other equivalent obligations of secrecy or to a code of professional ethics supervised and enforced by professional bodies, 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[495]

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 be subject to the control of an independent supervisory authority which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

---

[494] DE and UK scrutiny reservation.

[495] MT, NL, AT and PT reservation.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS[496]

(1) 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 **39a(7)**, [Article 43(3)], (…), Article **79a(4)**, 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), **(…)** 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.

[496] COM reservation on the deletion of empowerments for delegated acts or implementing acts.

5. A delegated act adopted pursuant to (…) Article 8(3), **(…)** Article **39a(7)**, [Article 43(3)], (…), Article 79a(4) **(…)** 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 89a

Relationship to previously concluded Agreements

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[497].

[497] COM reservation based on strong legal doubts on the legality of such proposal. COM refers to recital 79. DK, IT, RO and UK scrutiny reservation.

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*