Analysis

Second version

The Proposed Data Protection Regulation: What has the Council agreed so far?

Steve Peers, Professor of Law, University of Essex, Twitter: @StevePeers

13 March 2015

Introduction

Back in January 2012, the Commission proposed a new data protection Regulation that would replace the EU's existing Directive on the subject. It also proposed a new Directive on data protection in the sphere of law enforcement, which would replace the current 'Framework Decision' on that subject.

Over three years later, there has been considerable progress on discussing these proposals. The European Parliament (which has joint decision-making power on both proposals) adopted its positions back in the spring of 2014. For its part, the EU Council (which consists of Member States' justice ministers) has been adopting its position on the proposed Regulation in several pieces. It has not yet adopted even part of its position on the proposed Directive.

For the benefit of those interested in the details of these developments, the following analysis presents a consolidated text of the five pieces of the proposed Regulation which the Council has agreed to date, including the two parts just agreed in March 2015. This also includes the parts of the preamble which have already been agreed. I have left intact the footnotes appearing in the agreed texts, which set out Member States' comments.

The underline, italics and bold text indicate changes from the Commission proposal. I have added a short summary of the subject-matter of the Chapters and Articles in the main text which have not yet been agreed by the Council.

For detailed analyses of some parts of the texts agreed so far, see the links to the blog posts.

The Council might always change its current position at a later point, and of course the final text of the new legislation will also depend on negotiations between the Council and the European Parliament.

Background documents

'Public sector' provisions, agreed by Dec. 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016140%202014%20INIT

Chapter IV, agreed by Oct. 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT

Rules on territorial scope, agreed by June 2014 JHA Council:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT

Rules on 'one-stop-shop', agreed by March 2015 JHA Council:

http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf

Rules on basic principles, agreed by March 2015 JHA Council:

http://data.consilium.europa.eu/doc/document/ST-6834-2015-INIT/en/pdf

Proposal from Commission:

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Position of European Parliament:

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201

Analysis of agreed territorial scope rules:

http://eulawanalysis.blogspot.co.uk/2014/06/reforming-eu-data-protection-law.html

Analysis of agreed 'privacy seals' rules:

http://eulawanalysis.blogspot.co.uk/2014/10/warning-eu-council-is-trying-to.html

Analysis of data protection supervision (one-stop-shop) rules:

http://eulawanalysis.blogspot.co.uk/2015/03/when-super-regulators-fight-one-stop.html

Analysis of rules on basic principles:

http://eulawanalysis.blogspot.co.uk/2015/03/basic-data-protection-principles-in.html

Annex

Text of the general data protection Regulation agreed so far by the Council

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,[1] 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.

---

1 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.

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

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

11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors (…), to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. (…)

To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any such person. (…).

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.

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 reasonably 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[2].

23a) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection.

23b) (…)

23c) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis

[2] FR suggested this sentence be deleted.

should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented, taking into account the respective data processing and ensuring that additional information for attributing the personal data to a specific data subject is kept separetly. The controller who processes the data shall also refer to authorised persons within the same controller. In such case however the controller shall make sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data[3].

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[4].

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, including[5] electronic, oral statement or, if required by specific circumstances, by any other 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[6]. In such cases it is sufficient that the data subject receives the information needed to give freely specific and informed consent when starting to use the service. **(…)**. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes,

---

3 COM, IE, IT, AT, SE, UK reservation and FR scrutiny reservation on two last sentences.

4 DE reservation. AT and SI thought the last sentence of the recital should be deleted.

5 HU and DE would prefer to distinguish electronic from written statements.

6 PL and AT reservation.

unambiguous consent should be granted for all of the processing purposes. It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. **Therefore data subjects give their consent to certain areas of scientific research**[7] when **in** keeping with recognised ethical standards for scientific research[8]. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose[9]. 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[10].

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[11]; 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.

---

7 DE proposal.

8 IT scrutiny reservation.

9 AT, BE, CZ, IE and FR scrutiny reservation; COM reservation.

10 UK, supported by CZ and IE, proposed adding: 'Where the intention is to store data for an as yet unknown research purpose or as part of a research resource [such as a biobank or cohort], then this should be explained to data subjects, setting out the types of research that may be involved and any wider implications. This interpretation of consent does not affect the need for derogations from the prohibition on processing sensitive categories of data for scientific purposes' .

11 The Presidency points out that this recital may have to be aligned to the definition of health data (Article 4(12)) to be agreed in the future.

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. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered as concerned supervisory authorities when the draft decision concerns only the controller. 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. (…)[12]. This concerns especially the use of personal data

12 COM reservation on deletion of the UN Convention on the Rights of the Child reference.

of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child[13].

30) Any processing of personal data should be lawful and fair. (…). It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data.[14] 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. (…). Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means[15]. 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.

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.

---

13 CZ and AT reservation.

14 DE suggested inserting the following sentence: 'Data processing for archiving and statistical purposes in the public interest and for scientific or historical purposes is considered compatible and can be conducted on the basis of the original legal basis (e.g. consent), if the data have been initially collected for these purposes'.

15 UK reservation: this was too burdensome.

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.

33) (…)

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. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent[16].

[16] COM, BE, DK, IE and FR, SE reservation. CZ thought the wording should be more generic.

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. (…). Some types of *data processing may serve both important grounds of public interest and the vital interests of the data subject as, for instance when processing is necessary for* humanitarian purposes, including for *monitoring*

epidemic and its spread or in situations of humanitarian emergencies, in particular in situations of natural disasters[17].

38) The legitimate interests of a controller including of a controller to which the data may be disclosed or of a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller[18]. (…) **At any rate the existence**[19] of a legitimate interest 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. (…)

38a) Controllers that are part of a group of undertakings **or institution affiliated to a central body**[20] **may** have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes**, including the processing of clients' or employees' personal data**[21]. The general principles for the transfer of personal data**, within a group of undertakings, to an undertaking located in a** third country **(…)** remain unaffected.

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

17 CZ, FR, SE and PL thought the entire recital was superfluous.
18 HU scrutiny reservation.
19 BE suggestion, supported by COM and FI.
20 NL and FI proposal.
21 NL and FI proposal.

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. (…).

40) The processing of personal data for other purposes than the purposes for which the data have been initially collected should be only allowed where the processing is compatible with those purposes for which the data have been initially collected. In such case no separate legal basis is required other than the one which allowed the collection of the data. (…) If the 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, Union law or Member State law may determine and specify the tasks and purposes for which the further processing shall be regarded as lawful. The further processing (…) for archiving purposes in the public interest or, statistical, scientific or historical (…) purposes (…) or in view of future dispute resolution[22] should be considered as compatible lawful processing operations. **The legal basis provided by Union or Member State law for the collection and processing of personal data may also provide a legal basis for further processing for other purposes if these purposes are in line with the assigned task and the controller is entitled legally to collect the data for these other purposes**[23].
In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, 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

22 ES pointed out the text of Article 6 had not been modified regarding dispute resolution.
23 DE proposal. FR, IT and UK scrutiny reservation.

subjects, and the existence of appropriate safeguards in both the original and intended processing operations. 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 and on his or her rights should be ensured, including the right to object, should be ensured. (…). Indicating possible criminal acts or threats to public security by the controller and transmitting these data to a competent authority should be regarded as being in the legitimate interest pursued by the controller[24]. However such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.[25]

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. 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, taking into account that that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation[26]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. 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

---

24 AT and PL reservation.

25 IE, SE and UK queried the last sentence of recital 40, which was not reflected in the body of the text. DE, supported by BE, CZ, IE, GR and PL, wanted it to be made clear that Article 6 did not hamper direct marketing or credit information services or businesses in general according to GR.

26 AT scrutiny reservation.

personal data should be explicitly be provided inter alia 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.

Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject's explicit consent.

42) Derogating from the prohibition on processing sensitive categories of data should also be allowed when provided for in Union or Member State law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where (…) grounds of public interest so justify, in particular *processing data* **in the field of employment law, social security and social protection law, including pensions**[27] **and** *for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators.*
This may be done for health purposes, including public health (…) 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 archiving in the public interest or 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.

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 or social care services* and systems including the processing by the management and central national health authorities of such data for the

[27] NL proposal.

purpose of quality control, management information and the general national and local supervision of the health or social care system, *and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health. 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. (…)*[28].

42b) *The processing of special categories personal data* (…) *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 for 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*[29].

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

[28] Moved from recital 122.
[29] Moved from recital 123.

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.

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 established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation (…). 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][30], 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*[31] *risk of prejudice to the rights and freedoms of individuals* (…).

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

---

30 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.

31 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.

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 processor**s**, 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 risk**s** 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[32].

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

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

(…) 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[33] 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

[33] DE scrutiny reservation, querying especially about the application of the rules of place of purchase in relation to Article 89a.

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[34].

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[35].

---

34 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.

35 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

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.

---

future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards.

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.[36] 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.

[36] 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.

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.

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. 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.

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. (…).

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, the processing of personal data, carried out by public authorities or private bodies acting in the public interest processing affecting data subjects on its territory or processing carried out by a controller **or processor** 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 substantially affect 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. It should cooperate with the other authorities that are concerned, because the controller **or processor** has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority to which such complaint has been lodged should also be a concerned supervisory 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 **and on what constitutes a relevant and reasoned objection**[37].

96b) The lead authority should be competent to adopt binding decisions regarding 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 concerned supervisory authorities in the decision-making process. In cases where the decisions is to reject the complaint by the data subject in whole or in part that decision should be adopted by the supervisory authority at which the complaint has been lodged.

[37] DE proposal; CZ and LU scrutiny reservation.

96c) The decision should be agreed jointly by the lead supervisory authority and the concerned supervisory authorities 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 or private bodies acting in the public interest. 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 private 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 without prejudice to the powers of prosecutorial authorities under national law, to bring infringements of this Regulation to the attention of the judicial authorities and/or engage in legal proceedings. **Such powers should also include the power to forbid the processing on which the authority is consulted[38].** 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

38 Further to FR suggestion in relation to Article 53(1b)(e).

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 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. The adoption of such legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

100) (…).

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 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.

105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities (…) 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 *concerned* supervisory authority or the Commission[39] requests that such matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a (…) majority of its

[39] HU reservation on the reference to the Commission.

members so decides or if so requested by any *concerned* supervisory authority or the Commission. The European Data Protection Board should also be empowered to adopt legally binding decisions in case of disputes between supervisory authorities. For that purposes it should issue, **in principle** with a two-third majority of its members, legally binding decisions in clearly defined cases where there are conflicting views among supervisory authorities in particular in the cooperation mechanism between the lead supervisory authority and *concerned* supervisory authorities 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 *concerned* supervisory authorities should be applied and mutual assistance and joint operations might be carried out between the *concerned* supervisory authorities 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 Chair. 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 **(…).** The Commission *and the European Data Protection Supervisor* 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.

110a) The European Data Protection Board should be assisted by a secretariat provided by the secretariat of the European Data Protection Supervisor. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation should perform its tasks exclusively under the instructions of, and report to the Chair of the European Data Protection Board. Organisational separation of staff should concern all services needed for the independent functioning of the European Data Protection Board.

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) Any natural or legal person has the right to bring an action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union (the "Court of Justice") under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the concerned supervisory authorities who wish to challenge them, have to bring action within two months of their notification to them, in accordance with Article 263 TFEU. Where decisions of the European Data Protection Board are of direct and individual concern to a controller, processor or the complainant, the latter may bring an action for annulment against those decisions and they should do so within two months of their publication on the website of the European Data Protection Board, in accordance with Article 263 TFEU. Without

prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning this person.

Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints[40]. 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. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and **should** 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 which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation.

Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[41], whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the European Data Protection Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.

---

40 GR reservation.

41 Case C-314/85

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[42].

122) (…)[43].

123) (…)[44].

124) National law or collective agreements **(including 'works agreements')**[45] 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 (…) 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 (…) 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

---

42 Moved from recital 18.
43 Moved to recital 42a.
44 Moved to recital 42b.
45 DE proposal.

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) (…)[46].

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[47]. 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.

---

46 Moved to recitals 126c and 126d.

47 OJ C 113, 13.5.2003, p. 2.

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[48].

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[49]. 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[50] 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[51].

126a) Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and

48 CZ reservation.
49 CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.
50 AT and SE scrutiny reservation.
51 CZ, DK, FI, FR, HU, MT, NL, PT, SE, SI and UK scrutiny reservation.

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[52] *provides further specifications on statistical confidentiality for European statistics.*

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. (...).

---

52 OJ L 87, 31.3.2009, p. 164–173.

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[53].

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[54].

[NOT YET AGREED: Article 2: Material scope]

[53] 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.

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

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[55].

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

Article 4

Definitions

For the purposes of this Regulation:

(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 to an identified or identifiable person (…)[56].

(13) 'main establishment' means[57]

---

55 UK reservation.

56 DE, supported by UK, proposed reinserting the following reference 'or can be attributed to such person only with the investment of a disproportionate amount of time, expense and manpower'.

57 AT remarked that, in view technological developments, it was very difficult to pinpoint the place of processing and , supported by ES, HU, PL expressed a preference for a formal

- 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 and the latter establishment has the power to have such decisions implemented , in this case the establishment having taken such decisions shall be considered as the main establishment[58].

- 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 to the extent that the processor is subject to specific obligations under this Regulation;

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

(19a) '*concerned* supervisory authority ' means

- a supervisory authority which is concerned by the processing because:

  a) the controller or processor is established on the territory of the Member State of that supervisory authority;

---

criterion, which referred to the incorporation of the controller (AT, PL). AT pointed out that such criterion would avoid the situation that, depending on the processing activity concerned, there would be a different main establishment and consequently a different lead DPA.

58 BE reservation.

59 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.

b) data subjects residing in this Member State are substantially[60] affected or likely to be substantially affected by the processing; or

c) the underlying complaint has been lodged to that supervisory authority.

(19b) "transnational processing of personal data" means either:

(a) processing which takes place in the context of the activities of establishment**s** in more than one Member State of a controller or a processor in the Union and the controller or processor is established in more than one Member State; or

(b) processing which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect[61] data subjects in more than one Member State.

(19c) "relevant and reasoned objection" means :

an objection as to whether there is an infringement of this Regulation or not, or, as the case may be, whether the envisaged action in relation to the controller or processor is in conformity with the Regulation. The objection shall clearly demonstrate[62] the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects[63] and where applicable, the free flow of personal data.

(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[64];

[NOT YET AGREED: other definitions in Article 4]

CHAPTER II

---

60 IE and UK would prefer the term 'materially'.

61 Several Member States thought that this should be clarified in recital: CZ, FI, HU, SE.

62 BE thought that this was a threshold too high.

63 IE thought that also risks to the controller should be covered.

64 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.

PRINCIPLES

Article 5

Principles relating to personal data processing

1. Personal data must be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject[65];

   (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 or *scientific*, statistical[66] or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes[67];

   (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…)[68];

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

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…); personal data

---

65 DE proposed adding "and non-discriminatory" and "taking into account the benefit of data processing within a free, open and social society". This was viewed critically by several delegations (CZ, ES, IE, IT, NL, PL).

66 FR thought Chapter III should contain specific rules for protecting personal data processed for statistical purposes; DE and PL thought statistical purposes should also be qualified by the public interest filter. DE, supported by SI, suggested adding: "if the data have initially been collected for these purposes".

67 Referring to Article 6(2), DE and RO queried whether this phrase implied that a change of the purpose of processing was always lawful in case of scientific processing, also in the absence of consent by the data subject. BG thought that the second part of the sentence was redundant in view of Article 6(2). BE queried whether the concept of compatible purposes was still a useful one. HU and ES scrutiny reservations on reference to Article 83. FR, opposed by BE, thought that health data could be processed only in the public interest.

68 COM reservation on the deletion of the data minimisation principle. AT, CY, DE, EE, FR, HU, PL, FI and SI preferred to return to the initial COM wording, stating 'limited to the minimum necessary'. DE, supported by PL, also suggested adding: "they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data". DK and UK were opposed to any furter amendments to this point

may be stored for longer periods insofar as the data will be processed for archiving purposes in the public interest or *scientific*, statistical, or historical purposes in accordance with Article 83 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[69];

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

(f) (…)

2. The controller shall be responsible for compliance with paragraph 1[70].

Article 6

Lawfulness of processing[71]

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[72]consent to the processing of their personal data for one or more specific purposes[73];

(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;

---

69 FR, NL and SK scrutiny reservation. SK indicated that the case of private archiving was still not addressed. BE, CZ and SE thought the last part of this sentence should be deleted.

70 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 FR, this rule on liability may be dealt with in the context of Chapter VIII.

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

72 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.

73 RO scrutiny reservation.

(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 or of another person;

(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[74] pursued by the controller or by a third party [75] 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. (…)[76] [77].

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[78].

---

74 FR scrutiny reservation.

75 Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, PL, SE, SK and UK. COM, IE, FR and PL reservation on this reinstatement.

76 Deleted at the request of BE, CZ, DK, IE, FR, MT, SE, SI, SK, PT and UK. COM, CY, DE, FI, GR and IT wanted to maintain the last sentence. FR scrutiny reservation. COM reservation against deletion of the last sentence, stressing that processing by public authorities in the exercise of their public duties should rely on the grounds in point c) and e).

77 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.

78 It was pointed out that the text of Article 6 may have an adverse effect on the collection of personal data under administrative, criminal and civil law collections by third country public authorities, in that Article 6 provides that processing 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 may only take place to the extent established in accordance with Union or Member State law. Compliance with the administrative, regulatory, civil and criminal law requirements of a third country incumbent on controllers that engage in commercial or other regulated activities with respect to third countries, or voluntary reporting of violations of law to, or cooperation with, third country administrative, regulatory, civil and criminal law enforcement authorities appear not be allowed under the current draft of Article 6 . The Presidency thinks this point will have to be examined in the future, notably in the context of Chapter I.

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 ncarried out in the public interest or in the exercise of official authority vested in the controller. 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, unless the data subject has given consent[79], inter alia[80]:

(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, in particular whether special categories of personal data are processed, pursuant to Article 9;

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

(e) the existence of appropriate safeguards[81].

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected **by the same controller**[82], 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]. Further processing for incompatible purposes on grounds of

---

79 DK, IT and PT scrutiny reservation; IT deemed this irrelevant to compatibility test.

80 DK, FI, NL, RO, SI and SE stressed the list should not be exhaustive.

81 BG, DE, SK and PL reservation: safeguards as such do not make further processing compatible. FR queried to which processing this criterion related: the initial or further processing. DE and UK pleaded for the deletion of paragraph 3a.

82 AT proposal.

83 COM, DE, FI, HU and IT pleaded for the deletion of (f).

84 ES, AT and PL reservation; DE, HU scrutiny reservation. BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to in recital

legitimate interests of the controller or a third party shall be lawful if these interests override the interests of the data subject[86].

5. (…)[87]

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous[88]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, in an intelligible and easily accessible form, using clear and plain language.

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. Prior to giving consent, the data subject shall be informed thereof[89].

4. (…)

Article 8

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

[90]

---

40. BE, supported by FR, suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

85 HU, supported by BG, FR, AT and SK, thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here. The Presidency refers to the changes proposed in ADD 1 to 17072/3/14 REV 3

86 AT and PL scrutiny reservation.

87 DE asked for reinserting this paragraph.

88 COM reservation related to the deletion of 'explicit' in the definition of consent.

89 IE reservation. The Presidency concurs with SE that the last sentence belongs rather in Article 14. To that end the Presidency has made some suggestions set out in ADD 1 to 17072/3/14 REV 3.

90 CZ, MT, ES, SI would have preferred to see this Article deleted.

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child[91], the processing of personal data of a child (…) shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law.

1a. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1(…)[92]].

4. **(…).**

Article 9

***Processing of special categories of personal data*[93]**

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.

2. Paragraph 1 shall not apply if one of the following applies and Article 6(1) is complied with[94]:

---

91 Several delegations (DE, HU, ES, FR, SE, SK, PT) disagreed with the restriction of the scope and thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.

92 DE, ES, FR, SE and UK suggested deleting this paragraph. CZ suggested adding "and for identifying that a service is offered directly to a child". DE, supported by BE and FR, suggested giving the EDPB the power to issue guidelines in this regard.

93 COM, DK, SE, AT and NL scrutiny reservation. SK thought the inclusion of biometric data should be considered.

94 FR, AT and IT reservation (possibly restrict it by referring to Article 6(3)a); they considered Article 9 is *lex specialis*. DE, DK, FI, SI and NL thought that the limitation to paragraph 1 was too restrictive. COM, UK and IT could also agree to the deletion of the reference to Article 6(1).

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

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union law or Member State law or a collective agreement pursuant to Member State law providing for adequate safeguards; or

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

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

(e) the processing relates to personal data which are manifestly made public by the data subject **or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject**[95]; or

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(g) processing is necessary for (…)[96] reasons of public interest, on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests; or

(h) processing[97] is necessary for the purposes of preventive or occupational medicine[98], for the assessment of the working capacity of the employee[99], medical

95 PL proposal, supported by SI and COM.

96 IT, AT, PL and COM reservation on deletion of 'important'; DK suggested adding 'in the public interest vested in the controller'.

97 HU suggested reinstating "of health data" here and in point (hb).

diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law ***100*** or pursuant to contract with a health professional[101] and subject to the conditions and safeguards referred to in paragraph 4[102]; or

(ha) (…)**;**

(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; or

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

(j) (…)[103]

3. (…)[104]

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 point (h) **(…)** of paragraph 2 when those data are processed by* or under the responsibility *of a (…) professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies **or** by another person also subject to an obligation of secrecy under **Union or** Member State law or rules established by national competent bodies*.

---

98 AT would like to see this deleted; BE pointed out this type of medicine practice is not (entirely) regulated by law under Belgian law and therefore the requirement of paragraph 4 is not met.

99 PL and AT would like to see this deleted.

100 COM, IE, PL scrutiny reservation.

101 FR, PL and IT reservation.

102 AT, DE and ES 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.

103 Deleted at the request of AT, COM, EE, ES, FR, HU, IT, LU, MT, PL, PT, RO and SK. BE, DE, NL and FI wanted to reintroduce the paragraph.

104 COM reservation on the deletion of paragraph 3 on delegated acts.

4a. **(…)**[105].

5. **Member States may maintain or introduce more specific provisions with regard to genetic data or health data. This includes the possibility for Member States to exclude further processing of these data or to introduce further conditions for the processing of these data**[106]**.**

Article 9a

Processing of data relating to criminal convictions and offences[107]

Processing of data relating to criminal convictions and offences or related security measures based on Article 6(1)[108] *may only be carried out either under the control of official authority (…) or when the processing is* (…) *authorised by Union law or Member State law providing for adequate safeguards* for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority[109].

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data **do not or do no longer** require the identification of a data subject by the controller, the controller shall not be obliged to **maintain or** 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[110]. This in particular applies to the processing of pseudonymised data.

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

---

105 Deleted further to the request from COM, BE, CZ, DK, GR, IE, MT, NL, SE, FI and UK scrutiny reservation.

106 DE proposal, supported by BE.

107 DE and HU would prefer to see these data treated as sensitive data in the sense of Article 9(1). EE and UK are strongly opposed thereto.

108 IT was opposed to this reference.

109 SI, SK reservation on last sentence.

110 AT, DE, FR, HU, PL and UK scrutiny reservation.

the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification[111].

CHAPTER III

[NOT YET AGREED: Sections 1 to 4 of Chapter III (rights of the data subject), including right of access, right to be forgotten]

SECTION 5
RESTRICTIONS

Article 21

Restrictions[112]

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[113] 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;

---

111 DK, RO, SE and SI scrutiny reservation; COM and FR reservation; FR wanted to replace this paragraph by "This article shall not apply where the controller organized, by himself or through a third party, the impossibility to identify the data subject".

112 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.

113 AT reservation.

(b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, safeguarding public security[114], 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

(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

[114] 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.

CONTROLLER AND PROCESSOR[115]

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[116], 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. (…)

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

---

115 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.

116 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.

processing activity being carried out and its objectives, [including minimisation and pseudonymisation[117]], 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[118] 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. (…)

Article 24

Joint controllers[119]

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

---

117 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.

118 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).

119 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.

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 (…).

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**[120] **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) (…)

120 HU, SE and UK reservation.

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

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

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

Article 26

Processor

1. (…).[121] 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[122].

1b. (…)[123].

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

---

121 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.

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

123 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.

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;

(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*[124], 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*[125] 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.

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) [126].

---

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

125 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.

126 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).

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. (…)[127]

Article 27

Processing under the authority of the controller and processor

(…)

Article 28

Records of categories of personal data processing activities[128]

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.

---

127 COM reservation on deletion.

128 AT scrutiny reservation.

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

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[129]

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)[130].

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

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

   (a) describe the nature of the personal data breach including, where possible and appropriate, the 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

---

129 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.

130 BE, AT and PL thought this paragraph should be deleted.

(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. (….)[131]

Article 32

Communication of a personal data breach to the data subject[132]

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

131 COM reservation on deletion.

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

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

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. (…)[133]

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 33

Data protection impact assessment [134]

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[135] 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

---

133 COM reservation on deletion.

134 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).

135 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.

disadvantage, the controller (…)[136] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…).

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[137] 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) (…)[138], 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) (…)[139].

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. [140]

2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact

---

136 COM reservation on deletion.

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

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

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

140 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.

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. [141]

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[142].

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[143].

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 (…)[144].

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[145], paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. (…)

---

141 CZ reservation.

142 FR scrutiny reservation.

143 HU thought this should be moved to a recital.

144 CZ and FR indicated that this was a completely impractical obligation; IE reservation.

145 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.

7. (…)

Article 34

Prior (…) consultation[146]

1. (…)

2. The controller (…)[147] 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..

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[148] 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

---

146 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.

147 COM and LU reservation on deleting processor.

148 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.

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 (…).

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 (…)[149].

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[150].

8. (…)

9. (…)

SECTION 4
DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller or the processor may, or where required by Union or Member State law shall,[151] 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

---

149 IE scrutiny reservation on deletion.

150 SE scrutiny reservation.

151 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).

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.

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 [152]

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;

(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

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

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[153] 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.

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[154].

---

153 CZ preferred this monitoring to be optional.

154 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.'

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.

Article 38a

Monitoring of approved codes of conduct[155]

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[156] 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;

---

155 AT, LU scrutiny reservation.

156 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.

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

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

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

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

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

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

Article 39

Certification[157]

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.

[157] 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[158].

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.

---

158 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[159]

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:[160]

   (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) 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;

---

159 AT, FR, LU scrutiny reservation.

160 BE scrutiny reservation.

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

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

(d) it 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[161]. *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.

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.

---

161 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.

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[162].

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[163].

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)[164].

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[165] [166] [167] [168]

---

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

163 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.

164 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.

165 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

Article 40

General principle for transfers

(…)

Article 41

Transfers with an adequacy decision[169]

1. A transfer of personal data to a third country or an international organisation may take place where the Commission[170] has decided that the third country, or a territory or one ore more specified sectors within that third country, or

---

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).

166 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.

167 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.

168 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.

169 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.

170 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.

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 (…)[171], 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 (…)[172];

[171] AT would have preferred including a reference to national security.

[172] 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[173] 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[174] 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.

3. The Commission, after assessing the adequacy[175] of the level of protection, may decide that a third country, or a territory or one or more specified sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. (…)[176]. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies)

---

173 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*.

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

175 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.

176 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.

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)[177].

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*[178] in accordance with the examination procedure referred to in Article 87(2)[179].

[177] 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.

[178] 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.

[179] 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[180].

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)[181].

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[182].

---

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

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

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

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. (…)

Article 42

Transfers by way of appropriate safeguards[183]

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**[184]; 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)[185]; or

---

183 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.

184 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.

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

(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

(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. (….)

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*[186]*. 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*[187] in accordance with the examination procedure referred to in Article 87(2)[188].

---

186 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.

187 AT thought an absolute time period should be set.

188 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[189]

1. The competent supervisory authority shall *approve*[190] *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;

---

189 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.

190 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.

(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;

(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[191];

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

(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;

(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[192];

(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[193]; and

---

192 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.

193 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.

(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.][194]

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).

[194] 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[195]

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[196] 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[197]; or

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

---

195 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.

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

197 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'.

(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

(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*[198], 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[199] 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.

---

198 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.

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

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[200].

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[201]. Member States shall notify such provisions to the Commission[202].

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. (…)

---

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

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

202 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.

Article 45

International co-operation for the protection of personal data[203]

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

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

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[204];

   (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. (…)

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1

INDEPENDENT STATUS

Article 46

Supervisory authority

---

203 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.

204 AT and FI thought this subparagraph was unclear and required clarification.

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

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.

[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[205]].

Article 47

Independence

1. Each supervisory authority shall act with complete independence in performing the duties[206] 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, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody[207].

3. (…)[208]

4. (…)[209]

5. Each Member State shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure

---

205 DE, FR NL, EE that thought that this paragraph could be moved to the final provisions.

206 GR scrutiny reservation.

207 IE reservation: IE thought the latter part of this paragraph was worded too strongly.

208 AT, BE, DE and HU would prefer to reinstate this text. CZ, EE and SE were satisfied with the deletion.

209 COM and DE, AT reservation on deletion of paragraphs 3 and 4.

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.

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 of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control[210] which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, 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 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[211].

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

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the law of the Member State concerned[212].

4. (…)

---

210 EE reservation.

211 Several delegations (FR, SE, SI and UK) thought that other modes of appointment should have been allowed for. FR (and RO) thought that a recital should clarify that "independent body" also covers courts.

212 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 and HU also suggest that rules in the event of death or invalidity be added (see, for example, Article 42(4) of Regulation (EC) No 45/2001) as well as referring to a procedure for the nomination of a representative in case the member is prevented from performing his or her duties. CZ, NO, SE see no need for paragraph 3

5. (…)[213].

Article 49

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for:

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

(b) the qualifications (…) required to perform the duties of the members of the supervisory authority[214];

(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 (…) less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms 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 and rules governing the cessation of employment;

(g) (…)[215].

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*, 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.

---

213 COM, DE and AT scrutiny reservation on deletion of paragraphs 4 and 5.

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

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

Article 50

Professional secrecy

(…)

SECTION 2
COMPETENCE, TASKS AND POWERS

Article 51

Competence

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State. (…)
2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent[216]. In such cases Article 51a does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[217]. (…).

Article 51a

Competence of the lead supervisory authority

1. Without prejudice to Article 51, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the transnational processing of this controller or processor in accordance with the procedure in Article 54a.
2. (…)

---

216 COM opposes the exclusion of private bodies from the one-stop mechanism, pointing to the example of cross-border infrastructure provided by private bodies in the public interest. AT, IE, FR and FI preferred to refer to ' processing carried out by public authorities and bodies of a Member State or by private bodies acting on the basis of a legal obligation to discharge functions in the public interest'.

217 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.

2a. By derogation from paragraph 1, each supervisory authority shall be competent to deal with a complaint lodged with it or to deal with a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

2b. In the cases referred to in paragraph 2a, the supervisory authority shall inform the lead supervisory authority without delay on this matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will deal with the case in accordance with the procedure provided in Article 54a. **In case the lead supervisory authority decides not to deal with it**, the supervisory authority which informed the lead supervisory authority **shall** deal with the case according to Articles 55 and 56 and **shall** submit**, within a period of three weeks following the decision of the lead supervisory authority,** to the **latter** authority a draft decision, which will be adopted according to paragraphs 4a, 4b, 4bb of Article 54a.

In case of disagreement between the supervisory authorities, the lead supervisory authority shall deal with the case in accordance with the procedure provided in Article 54a.

3. The lead supervisory authority shall be the sole interlocutor of the controller or processor for their transnational processing.

4. (…).

Article 51b

Identification of the supervisory authority competent for the main establishment

(…)

Article 51c

One-stop shop register

(…)[218]

[218] AT reservation on the deletion of Articles 51b and 51c.

Article 52

Tasks [219]

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

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

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

(ab) 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[220];

(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 lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73, and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period , 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;

---

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

220 NL reservation.

(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;

(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);

(ga) encourage the drawing up of codes of conduct pursuant to Article 38 and give an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 38 (2);

(gb) promote the establishment of data protection certification mechanisms and of data protection seals and marks, and approve the criteria of certification pursuant to Article 39 (2a)**;**

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

(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. (…).

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. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[221].

Article 53

Powers[222]

1. Each Member State shall provide by law that its supervisory authority shall have at least[223] 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[224];

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

   (b) (…)

   (c) (…)

---

221 DE, NL and SE reservation: this could be left to general rules.

222 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.

223 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.

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

(d) to notify the controller or the processor of an alleged infringement of this Regulation[225];

(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[226] to a controller or processor where processing operations have infringed provisions of this Regulation[227];

(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;

(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 **(…)**[228];

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

---

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

226 PL and SK scrutiny reservation.

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

228 Moved to recital 99.

(g) to impose an administrative fine pursuant to Articles 79 and 79a[229], 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[230],

(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), if the law of the Member State requires such prior authorisation;

(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;

(ae) to issue certifications and approve criteria of certification in accordance with Article 39(2a);

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

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

(ca) to authorise administrative agreements referred to in point (d) of Article 42 (2a);

(d) to 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*

---

229 DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.

230 NL scrutiny reservation.

and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.[231]

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[232], in order to enforce the provisions of this Regulation[233].

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.

CHAPTER VII[234]
CO-OPERATION AND CONSISTENCY
SECTION 1
CO-OPERATION

Article 54a

Cooperation between the lead supervisory authority and other concerned supervisory authorities [235]

1. The lead supervisory authority (…) shall cooperate with the other concerned supervisory authorities in accordance with this article in an endeavour to reach

---

231 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.

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

233 DE thought para. 3 should be deleted.

234 AT and FR scrutiny reservation on Chapter VII.

235 BE, CZ, CY, DE, EE, FR, FI, IE, LU, RO, PT and NL scrutiny reservation.

consensus (…). The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other.

1a. The lead supervisory authority may request at any time other concerned supervisory authorities 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.

2. The lead supervisory authority shall, without delay communicate the relevant information on the matter to the other concerned supervisory authorities. It shall without delay submit a draft decision to the other concerned supervisory authorities for their opinion and take due account of their views.

3. Where any[236] of the other concerned supervisory authorities within a period of four weeks after having been consulted in accordance with paragraph 2, expresses a relevant and reasoned objection *to the draft decision*, the lead supervisory authority shall, if it does not follow the objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 57. (…)

3a. Where the lead supervisory authority intends to follow the objection made, it shall submit to the other concerned supervisory authorities a revised draft decision for their opinion. This revised draft decision shall be subject to the procedure referred to in paragraph 3 within a period of two weeks.

4. Where none of the other concerned supervisory authority has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 3 and 3a, the lead supervisory authority and the concerned supervisory authorities shall be deemed to be in agreement with this draft decision and shall be bound by it.

4a. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other concerned supervisory authorities and the European Data Protection Board of the decision in question including a summary of the

---

236 A number of Member States (CZ, IE, NL, PL, FI and UK) still prefers a quantitative threshold by which an objection would need to be supported by 1/3 of the concerned supervisory authorities before the lead authority is obliged to refer the matter to the EDPB.

relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

4b. By derogation from paragraph 4a, where a complaint is dismissed or rejected, the supervisory authority to which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

4bb. Where the lead supervisory authority and the concerned supervisory authorities are in agreement to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State **and shall inform the complainant thereof**[237], while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint and notify it on that complainant[238] **and shall inform the controller or processor thereof**. [239]

4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a and 4bb, 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 inform the other concerned supervisory authorities .

4d. Where, in exceptional circumstances, a concerned supervisory authority 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 other concerned supervisory authorities shall supply the information required under this Article (…) to each other by electronic means, using a standardised format.

Article 54b

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

---

237 Further to suggestions from HU and IE.

238 SI scrutiny reservation. PL reservation on paras 4b and 4bb: PL and FI thought para. 4bb should be deleted as it was opposed to the concept of a split decision. IT thought para 4bb overlapped with para 4b.

239 Further to suggestions from HU and IE.

(…)

Article 55

Mutual assistance[240]

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[241] 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[242], including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. 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[243]; 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

---

240 DE, NL SE and UK scrutiny reservation.

241 ES, supported by PT, had suggested 15 days. RO and SE found one month too short. COM indicated that it was only a deadline for replying, but that paragraph 5 allowed longer periods for executing the assistance requested.

242 EE and SE scrutiny reservation.

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

to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request[244].

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means[245], 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[246].

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[247] 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[248].

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months[249]. 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)[250].

---

244 RO scrutiny reservation.

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

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

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

248 EE, FR, RO and UK reservation. DE scrutiny.

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

250 DE, IT, EE, CZ and NL reservation.

Article 56

Joint operations of supervisory authorities[251]

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[252] 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 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.

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. (…) [253]

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

---

251 DE, EE, PT and UK scrutiny reservation.

252 COM reservation; IT, supported by FR, BE and CZ suggested stressing the multilateral aspect by adding text.

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

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[254].

4. (…)

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

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

SECTION 2

CONSISTENCY[255]

Article 57

Consistency mechanism[256]

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[257].

---

254 UK reservation on paras. 3a, 3b and 3c.

255 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.

256 EE, FI, NL and UK scrutiny reservation.

257 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 decision to the European Data Protection Board, when it:

(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 at approving 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 at determining standard data protection clauses referred to in point (c) of Article 42(2); or

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

(f) aims at approving binding corporate rules within the meaning of Article 43.

3. The European Data Protection Board shall adopt a binding decision in the following cases:

a) Where, in a case referred to in paragraph 3 of Article 54a, a *concerned* supervisory authority has expressed a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant and/or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of the Regulation;

b) Where, there are conflicting views on which of the *concerned* supervisory authorities is competent for the main establishment;

c) (…)

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 follow the opinion of the European Data Protection Board issued under Article 58. In that case, any concerned supervisory authority or the Commission may communicate the matter to the European Data Protection Board.

4. 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, in particular 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.

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 decision, the grounds which make the enactment of such measure necessary, and the views of other *concerned* supervisory authorities.

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[258]

1. (…)

2. (…)

3. (…)

4. (…)

258 NL and UK scrutiny reservation.

5. (…)

6. (…)

7. In the cases referred to in paragraphs 2 and 4 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. 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.

7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft decision 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 4 of Article 57 and the Commission of the opinion and make it public.

8. The supervisory authority referred to in paragraph 2 of Article 57 shall take utmost 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 decision and, if any, the amended draft decision, using a standardised format.

9. Where the concerned supervisory authority 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 **3** of Article 57 shall apply.

10. (…)

11. (…)

Article 58a

Decisions by the European Data Protection Board[259]

1. In the cases referred to in paragraph 3 of Article 57, the European Data Protection Board shall adopt a decision on the subject-matter submitted to it in order to ensure the correct and consistent application of this Regulation in individual cases. The decision shall be reasoned and addressed to the lead supervisory authority and all the concerned supervisory authorities and binding on them.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter.

3. In case the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board[260]. In case the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The concerned supervisory authorities shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. (…)

The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 to the concerned supervisory authorities. It shall inform the Commission thereof. The decision shall be published on the website of the European Data Protection Board without delay after the supervisory authority has notified the final decision referred to in paragraph 7.

---

259 PL scrutiny reservation. IE thought the controller should have standing to intervene in the proceedings before the EDPB.

260 AT and HU reservation. HU believes that this option will make the general two-thirds majority rule meaningless and symbolic, since there will be no effective incentive for the EDPB to adopt a decision that reflects the view of the vast majority of DPAs of the Member States, as eventually every decision could be adopted by only a slight majority of them. It would also undermine the general validity of the EDPB's decision, since the fact that the Board could not come to an agreement on a particular matter supported by at least the two-thirds of its members might give rise to serious doubts whether the finding of such decision is commonly shared across the Union.

6. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged shall adopt their final decision on the basis of the decision referred to in paragraph 1[261], without undue delay and at the latest by one month after the European Data Protection Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged, shall inform the European Data Protection Board of the date when its final decision is notified respectively to the controller or the processor and the data subject. The final decision of the concerned supervisory authorities shall be adopted under the terms of Article 54a, paragraph 4a, 4b and 4bb. The final decision shall refer to the decision referred to in paragraph 1 and shall specify that the decision referred to in paragraph 1 will be published on the website of the European Data Protection Board in accordance with paragraph 6. The final decision shall attach the decision referred to in paragraph 1.

Article 59

Opinion by the Commission[262]

(…)

Article 60

Suspension of a draft measure[263]

(…)

Article 61

Urgency procedure[264]

1. In exceptional circumstances, where a **concerned** [265] supervisory authority considers that there is an urgent need to act in order to protect rights and freedoms of data

---

261 FI reservation; would prefer a system under which the EDPB decision would be directly applicable and would not have to be transposed by the lead DPA.

262 COM and FR reservation on deletion.

263 COM and FR reservation on deletion.

264 DE scrutiny reservation.

265 Further to BE suggestion.

subjects, it may, by way of derogation from the consistency mechanism referred to in Article 57[266] or the procedure referred to in Article 54a, immediately adopt provisional measures intended to produce legal effects within the territory of its own Member State[267], with a specified period of validity. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the **other** concerned supervisory authorities, the European Data Protection Board and to the Commission.

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

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 a 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 decision, 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 binding decision 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) (…)[268];

(b) (…);

(c) (…);

---

266 HU remarked that it should be clarified whether provisional measures can be adopted pending a decision by the EDPB. The Presidency thinks that the reference to Article 57 makes it clear that this is indeed possible.

267 COM scrutiny reservation.

268 COM reservation on deletion.

(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).

2. (…)

3. (…)

Article 63

Enforcement

(…)

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64

European Data Protection Board

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 of one supervisory authority of each Member State or his/her representative ~~and of the European Data Protection Supervisor~~.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, (…) a joint representative shall be appointed in accordance with the national law of that Member State.

4. The Commission **and the European Data Protection Supervisor or his/her representative** shall have the right to participate in the activities and meetings of the European Data Protection Board *without voting right*. **The Commission** shall designate a representative. The chair of the European Data Protection Board shall,

communicate to the Commission ~~the details of~~ the activities of the European Data Protection Board.

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.[269]

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[270].

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(3) 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[271];

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

---

269 UK and SI scrutiny reservation.

270 DE scrutiny reservation.

271 DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.

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

(cb) 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[272];

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

(ce) give the Commission an opinion on the level of protection of personal data 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 4 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) (…);

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

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,

[272] 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.

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 binding decisions referred to in paragraph 3 of Article 57.

Article 68

Procedure

1. The European Data Protection Board shall adopt binding decisions referred to in paragraph 3 of Article 57 in accordance with majority requirements set out in paragraphs 2 and 3 of Article 58a. As regards decisions related to the other 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.

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairs from amongst its members **by simple majority**[273](…)[274].

2. The term of office of the chair and of the deputy chairs shall be five years and be renewable once[275].

---

273 IE proposal.

274 COM reservation on deletion.

[275] NL thought that the Regulation should also address the case where a chair or a deputy chairperson ceases to be a member of the EDPB. However, this may be left to national law of the Member state concerned. COM scrutiny reservation.

Article 70

Tasks of the chair

1. The chair shall have the following tasks:

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

   (aa) to notify decisions adopted by the European Data Protection Board pursuant to Article 58a to the lead supervisory authority and the *concerned* supervisory authorities;

   (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, **which shall be provided** by the secretariat of the European Data Protection Supervisor (…).

1a. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the European Data Protection Board.

1b. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation shall be organizationally separated from, and subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor[276].

1c. Where needed, the European Data Protection Board in consultation with the European Data Protection Supervisor shall establish and publish a Code of Conduct implementing this Article and applicable to the staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation.

[276] CZ reservation on last part of the task.

2. The secretariat shall provide analytical[277], administrative and logistical support to the European Data Protection Board.

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, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the European Data Protection Board.

Article 72

Confidentiality[278]

1. The discussions[279] 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.

---

277 UK suggested deleting "analytical".

278 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.

279 IT scrutiny reservation: it suggested replacing this term with 'minutes' or 'summary records', thereby distinguishing between confidentiality of decision-making and access to documents.

[NOT YET AGREED:

Chapter VIII: Remedies, Liability and sanctions]

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[280] 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)[281] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (…).

Article 80a

Processing of personal data and public access to official documents [282]

Personal data in official documents held by a public authority or a public body or a private

---

280 HU, AT, SI and SE reservation; they would prefer not to limit this paragraph to journalistic processing.

281 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.

282 SK and PT scrutiny reservation.

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*[283].

Article 80b [284]

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

(…)[285]

---

283 COM reservation in view of incompatibility with existing EU law, in particular Directive 2003/98/EC (as amended by Directive 2013/37/EU).

284 DK, PL, SK scrutiny reservation.

285 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

Article 81a

Processing of genetic data

(…)[286]

Article 82

Processing in the employment context

1. Member States may by law or by collective agreements, provide for more specific[287] 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[288].

Article 82a

---

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.

286 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.

287 DE, supported, by AT, CZ, HU, DK and SI, wanted to refer to 'stricter' rules.

288 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.

Processing for purposes of social protection

(…)

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[289] 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[290], 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[291].

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.

---

289 PL and SI would want to restrict this to statistical processing in the public interest.

290 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.

291 COM and AT thought the list of articles from which can be derogated should be more limited.

3. (…).

Article 84

Obligations of secrecy [292]

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[293]

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.

---

292 DE and UK scrutiny reservation.

293 MT, NL, AT and PT reservation.

[NOT YET AGREED:

Chapter X: Delegated Acts and Implementing Acts

Chapter XI: Final Provisions]
