COUNCIL OF THE EUROPEAN UNION

Brussels, 27 March 2013

8004/13

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 35
JAI 246
MI 246
DRS 59
DAPIX 65
FREMP 35
COMIX 217
CODEC 688

NOTE

from:	Presidency
to:	Working Party on Data Protection and Exchange of Information
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
No. prev. doc.:	16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155 5779/13 DATAPROTECT 4 JAI 53 MI 47 DRS 18 DAPIX 8 FREMP 4 COMIX 44 CODEC 164 6607/13 DATAPROTECT 18 JAI 125 MI 116 DRS 30 DAPIX 28 FREMP 13 COMIX 108 CODEC 359
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Revised version of Chapters I-IV

1. At the end of January, the Presidency finalised the first examination of the entire draft Regulation. Since then, further discussions have taken place, notably on introducing a more risk-based approach and more flexibility for the public sector into the text of the Regulation. Both items were also discussed at the JHA Council meeting of 7-8 March 2013.

2. The Working Party on Data Protection and Exchange of Information (DAPIX) also engaged in further discussions on the right to be forgotten, the right to data portability and profiling as well as on pseudonymisation and certification.

3. The Presidency has based itself on these discussions to revise the text of Chapters I to IV of the draft regulation. Obviously any changes made are *ad referendum,* subject to further scrutiny by all delegations (including the Commission).

4. The Presidency has sought to incorporate these changes into the revised draft of the Regulation issued at the end of the Cyprus Presidency. As the changes introduced into that document had not yet been discussed, the underlined text has been kept. New changes are indicated in underlined bold text.

5. The entire preamble has been reproduced in the annex, but only the recitals pertaining to Chapters I to IV should be discussed.

6. All delegations have a general scrutiny reservation on this proposal and the following delegations have a parliamentary scrutiny reservation: CZ, HU, NL, PL and UK. Several delegations have a reservation on the chosen legal form of the proposed instrument and would prefer a Directive[1].

7. The Presidency invites the Working Party to commence the second examination of Chapters I -IV.

---

[1] BE, CZ, DK, EE, HU, LT, SE, SI and UK. DE thinks that a Regulation, in the currently proposed form, is not the right solution to regulate data protection in the Member States' public sector. LT would prefer one instead of two legal acts and regulate data protection in all areas through a directive**.**

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[3],

After consulting the European Data Protection Supervisor[4],

Acting in accordance with the ordinary legislative procedure,

---

[2] The Presidency deleted the reference to Article 114 TFEU, as it saw no need for a double legal basis for this proposal, which can be based in its entirety on Article 16 TFEU. IT reservation.

[3] OJ C, p. . .

[4] OJ C p. .

Whereas:

1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.

2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.

3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

3a) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity[6].

---

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

[6] The Presidency has moved former recital 139 up here so as to emphasise the importance of the fundamental rights dimension of data protection in connection with other fundamental rights.

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

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

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

7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

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

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

11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. 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 person. This should also apply where the name of the legal person contains the names of one or more natural persons.

13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.

14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, **taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union** (…) or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

14a) This Regulation does not cover the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/200[17] and other Union legal instruments **applicable to the** such processing of personal data should be adapted to the principles and rules of this Regulation **(…).**

15) This Regulation should not apply to processing of personal data by a natural person, which are (…) personal or domestic, (…) and thus without any connection with a professional or commercial activity. **However, this Regulation** should (…)apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

---

7 OJ L 8, 12.1.2001, p. 1.

16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY)[8]. **When processing of personal data by public authorities or by private entities falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering and activities of administrative police.**

17) **Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation.** This Regulation should **therefore** be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Personal data in documents held by a public authority or a public body may be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject, and the data subject's legitimate interests or fundamental rights and freedoms in the particular case are not prejudiced.

---

[8] ES had proposed to add a recital on the processing of personal data by authorities that are competent for drawing up electoral rolls.

19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects **irrespective of whether connected to a payment or not,** or to the monitoring of the behaviour of such data subjects **, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficent 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 to such data subjects in the Union**[9], or to the monitoring of the behaviour of such data subjects.

[9] Presidency proposal aimed at narrowing/clarifying the scope of Article 3(2)(a).

21) 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[10].

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[11] in a Member State's diplomatic mission or consular post.

23) The principles of **data** protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. **To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, considering both the state of the art in technology at the time of the processing and technological development.** The principles of data protection should therefore not apply to anonymous information which do 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[12]. The principles of data protection should not apply to deceased persons[13].

---

10 UK suggests deleting this recital.
11 UK queries whether the words 'such as' imply that there are other examples and, if so, which.
12 Presidency clarification regarding the fact that anonymous data are not covered by the Regulation.
13 Suggested clarification in accordance with a SE suggestion.

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, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. However, identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances[14].

25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data[15]. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

---

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

15 UK suggests deleting 'including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data'.

(25a) **Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired during early prenatal development 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[16].**

26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including **genetic data and** biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.

[16] New recital in order to clarify the definition of Article 4 (10)

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. (…)[17].

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. T**he particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means.

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

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.

33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.

34) **In order to safeguard that consent has been given freely, c**onsent 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 that specific situation**. (…)[18]

35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

[18] Deleted as Article 7(4) was also deleted by the Presidency.

36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law or in a Member State law. (…). It **should be** also for Union or national law to determine **the purpose of the processing . Furthermore, this legal basis could, within the limits of this Regulation, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.**

37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.

38) The legitimate interests of a controller including of a controller to which the data may be disclosed may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. I n particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object **to** the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the exercise of their public duties.

39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. The processing of personal data to the extent strictly necessary for the purposes of preventing and monitoring fraud also constitutes a legitimate interest of the data controller concerned[19]. **The processing of personal for the purposes of anonymising or pseudonymising personal data also constitutes a legitimate interest of the data controller concerned.**

40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific (…) purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.

[19] BE proposal.

41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific (…) purposes.

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

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

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

46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This information could be provided in electronic form, for example, when addressed to the public, through a website[20]. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.

47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, without unreasonable charge, in particular access to data, rectification, erasure and to exercise the right to object. **Thus the controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means**[21].The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.

48) The principles of fair and transparent processing require that the data subject should be informed (…) of the existence of the processing operation and its purposes (…). The controller should provide the data subject with any further information necessary to guarantee fair and transparent processing. Furthermore the data subject should be informed on (…) measures based on profiling, as well as the consequences of such operations and measures on individuals[22]. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

---

20 Further to suggestion by BE.

21 Language moved from Article 12(1a) and made more flexible as ES and DE pointed out that there should be no causal link between the automatic processing of data and the possibility to make requests in an electronic form and the criticism voiced by BE, CZ, ES and UK that this requirement was not technology neutral. CZ thought the form of communication should be agreed between the data controller and data subject.

22 NL proposal aimed at emphasising that transparency is a key value in accepting and accommodating profiling operations, while at the same time strengthening data subjects rights.

49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

50) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific (…) purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic involved in any automatic data processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates[23].

[23] Further to ES suggestion.

52) The controller should use all reasonable measures to verify the identity of a data subject **who** requests access, in particular in the context of online services and online identifiers. **However, 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 the request for access.** A controller should not retain personal data for the **sole** purpose of being able to react to potential requests.

53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is in particular relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific (…) purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform **the controllers** which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, **taking into account the state of the art and the means available to the controller,** including technical measures, in relation to data for the publication of which the controller is responsible. **(…).**

54a) Methods to **restrict processing of** personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data unavailable to users or temporarily removing published data from a website. **In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted[24].**

55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.

[24] Moved from Article 17a, paragraph 2.

58) Every **data subject** should have the right not to be subject to a decision which is based on profiling (…). However, such measure should be allowed when expressly authorised by **Union or Member State** law, including for **fraud monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or** carried out in the course of entering or performance of a contract between the data subject and **a** controller[25], or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention (…). **Profiling for direct marketing purposes or based on special categories of personal data should only be allowed under specific conditions**.

59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[25] BE proposal.

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 to ensure and be able** to demonstrate the compliance of each processing operation with this Regulation**, taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, such as excluding individuals from their rights or from the control over their personal data or giving rise to discrimination, identity theft or fraud, financial loss, damage of reputation or any other economic or social disadvantage. Where personal data are processed on behalf of the controller, the implementation of such measures should include in particular to use only a processor providing sufficient guarantees to implement appropriate technical and organisational measures. Where the processing is likely to represent specific risks for the rights and freedoms of data subjects, the controller or processor should carry out, prior to the processing an assessment of the impact of the envisaged processing operations on the protection of personal data. Guidance for the implementation of such measures by the controller could be given in particular by approved codes of conduct, approved certifications or guidelines of the European Data Protection Board, by a data protection officer, or, where a data protection impact assessment indicates that processing operations involve a high degree of specific risks, by the consultation of the supervisory authority prior to the processing. If proportionate, the verification of the obligations of the controller may be carried out by independent internal or external auditors or by providing an approved certification**[26].

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

---

[26] BE reservation.

62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority. **The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance of the controller.**

64) (…).

(64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to present specific risks, the controller or the processor shall be responsible to perform a data protection impact assessment. The outcome of the assessment shall be taken into account when determining the extent of the requirements, in particular when implementing appropriate measures to ensure and be able to demonstrate that the processing of personal data is in compliance with this Regulation[27].

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 risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

[27] Further to NL proposal.

67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred **in processing operations where there is a risk that the data subjects' rights or legitimate interests will be severely affected, in particular in the case of identity theft or fraud, damage to reputation or any other significant economic or social disadvantage**[28], the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

[28] DE proposal. NL thought it was better to refer to the data protection impact assessment as criterion for selection data breaches to be notified.

68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, **the controller must**[29] ascertain whether **all** appropriate technological protection and organisational measures **have been implemented**[30] to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

(68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data and using pseudonymous data.

69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

[29] NL proposal
[30] NL proposal

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes **including in the case of identity theft; substantive financial loss of the data subject or third party; loss of confidentiality of bank or creditcard account numbers of the data subject or third party; discrimination of the data subject or third party, loss of confidentiality of data protected by a professional secrecy regulated by Union or Member State law, moral damage to the data subject or third party**[31]. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to newly established large scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

73) Data protection impact assessments should 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.

---

31 Further to NL proposal.

74) Where a data protection impact assessment indicates that **the** processing **is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks and freedoms of individuals**, a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right**s or giving rise to unlawful or arbitrary discrimination, substantial identity theft, , significant financial loss, significant damage of reputation or any other significant economic or social damage,** or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of **the processing activities. The supervisory authority should make recommendations to remedy a situation where the envisaged processing** might not be in compliance with this Regulation. **The supervisory authority should respond to the request for consultation in a defined period, during which the controller or processor shall not commence processing activities. After that period the controller or processor should be allowed to start the intended processing activities under its own responsibility even in the absence of a reaction of the supervisory authority. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its duties and powers laid down in this Regulation**. Such consultation should equally take place in the course of the preparation of a **legislative or regulatory** measure which **provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing**.

75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which **require regular and systematic monitoring,** a person **with expert knowledge 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 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 callibrate the obligations of controllers and processors, taking into account the risks inherent to the processing for the rights and freedoms of data subjects**

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 are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.

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

80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation. The existence of mutual binding obligations of professional secrecy, such as the professional secrecy of the medical and legal professions, or binding special sectoral legislation which protects the interests of data subjects, such as common in the financial sector, may also be used[32].

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

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, 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.

[32] NL proposal.

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, processors and processors and sub-processors to include the standard data protection clauses in a wider contract nor to add other clauses 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. In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses[33].

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

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

87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.

---

[33] BE proposal.

88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific (…) purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

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

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

91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.

92) The establishment of supervisory authorities in Member States, exercising their functions with [complete] independence, is an essential component of the protection 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[34].

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

94) Each supervisory authority should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.

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

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

97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

98) The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.

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

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

101) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

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

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

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

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

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

107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.

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

109) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.

112) Any body, organisation or association which aims to protects 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 should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.

113) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established.

114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.

115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.

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

117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.

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

119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.

120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. 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 and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

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

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

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

(124a) As regards statistics, Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities[35] provides further specifications on statistical confidentiality for European statistics.

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

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

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

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

---

[35] OJ L 87, 31.3.2009, p. 164–173.

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

130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers36. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

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

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

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

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

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

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

136) (…).

137) (…)[37].

138) (…)[38].

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

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

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals[39] with regard to the processing of personal data and rules relating to the free movement of personal data[40].

2. This Regulation protects (…)[41] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. [**Any restriction on** the free movement between **Member States** of **personal data** shall be prohibited**, unless the processing of such data is not in accordance with this Regulation**] [42] [43] [44].

---

39 AT, supported by LI, thought that a recital should acknowledge Member States' right to lay down the right to data protection rules for legal persons.

40 IT thought that a reference to the internal market should be added here. DE, on the other hand, thought that it was difficult to determine the applicability of EU data protection rules to the public sector according to internal market implications of the data processing operations.

41 Deletion of 'the' in order to allay concerns that this paragraph conveyed the impression that the right to data protection enjoyed a higher status than other fundamental rights.

42 FR thought that this paragraph, which was copied from the 1995 Data Protection Directive (1995 DPD 95/46), did not make sense in the context of a Regulation as this was directly applicable. NL remarked that the drafting did not specify the addressees of this rule. DE scrutiny reservation: queried whether Member States would still be allowed to keep more stringent, sectoral data protection rules in place. SK thought that this paragraph needed to be redrafted so as to allow processing of personal data from one Member State in another Member State, also in cases where the processing in another Member State was not necessary or reasonable.

43 EE, FI, SE, and SI thought that the relation to other fundamental rights, such as the freedom of the press, or the right to information or access to public documents should be explicitly safeguarded by the operative part of the text of the Regulation. FI thought that Member States should retain the right to apply their national legislation in this regard. DE concurred that this was a very important issue which needed to be addressed. The Commission stated that its proposal did not contain rules on the access to public documents as regards the fundamental right aspect, since the Charter only refers thereto regarding the EU institutions.

44 The Presidency invites the Council Legal Service to express a view on this text.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system[45] [46].

2. This Regulation does not apply to the processing of personal data:[47]

   (a) in the course of an activity which falls outside the scope of Union law (…)[48];

   (b) by the Union institutions, bodies, offices and agencies[49];

   (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union[50];

---

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

46 BE scrutiny reservation related to the fact that the processing of personal data by judicial authorities would be covered by the Directive.

47 The Presidency considers that a specific exclusion for data which have been rendered anonymous may be beneficial.

48 DE, RO and SI thought the activities covered by Union law should be listed as fully as possible. SE also thought that the utmost clarity was required in this respect. The Presidency is of the opinion that activities which fall outside the scope of Union law such as processing operations concerning public order, internal security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) should rather be clarified in a recital.

49 FR wants clarification as to whether transfers of data by Member States to these EU institutions are covered by this exception. BE, DE, EE, ES and RO thought the Regulation should be applicable to EU institutions.

50 IT thought this exception overlapped with (a).

(d) by a natural person (…)[51] in the course of (…) a personal or household activity;

(e) by competent **public** authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[52] [53].

3. (…)[54].

---

[51] Deleted further to the remarks by DE, IE, LT, NL, SI and UK, who questioned the need for the criterion of absence of gainful interest in this so-called household exception and the compatibility thereof with the Lindqvist case law of the ECJ (which, at any rate, predated the 'social network era'). UK thought that selling personal possessions on an auction site also fall within the household exemption. The enforceability of data protection rules in this type of situation was also challenged. SE thought the household exception needed to be drafted in a sufficiently wide manner so as to ensure the practical enforceability of data protection rules. COM affirmed the compatibility with the Lindqvist case law. Several delegations (DE, SE, SI and UK) asked whether the use of social networks on the internet would be covered by this exception. COM replied that in its view the Regulation should apply to an individual who uses a social network and has 'with the public' privacy settings, i.e. when personal data are available itch to an unrestricted number of individuals and not only to a limited audience. CZ thought that the processing of personal data by a natural person which is not part of its own gainful activity should be subjected to limited, specific rules to be spelled out in the Regulation. LU, NO, SI and SK also thought this exception needed to be more clearly regulated. LT proposed to add 'with the exception of data which might be made available to transfer to third parties or publish'. BE, supported by RO, would like to add the following recital: 'That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.'

[52] RO scrutiny reservation: it thought that this exception should be worded more broadly and suggested referring to 'competent authorities for the purpose of ensuring public order and security'. FR thought that this exception should be worded more broadly so that it would cover all forms of exercise of 'sovereign power' with a sanctioning goal. FR also thought that the 'competent authorities' should be clearly defined. COM replied that point e) should mark the delimitation between the two data protection instruments. DE referred to the difficulties flowing from the fact that the prevention of dangerous situations (*Gefahrenabwehr*) is not covered by the proposed Data Protection Directive, whereas the processing of data in that context is intrinsically linked to other police activities covered by that Directive. At the request of HU, COM clarified that Member States in their national data protection legislation could cover in a single law also data processing in this area.

[53] ES proposed to insert two further exemptions for processing by competent authorities for the purposes of producing and disseminating official statistics and of drawing up electoral rolls.

[54] Moved to recital 17. FR demands clarification as to whether 'Business to Business (B2B)' transactions are covered by the proposed Regulation. FR and IT underlined the importance of close alignment of this Regulation with the E-Commerce Directive; IT thought that it was not expedient that the exceptions listed here were broader than under the E-Commerce Directive. DE queries whether also the implementing law of the Member States should be taken into account or also other EU Directives, such as Directive 2002/58/EC.

Article 3

Territorial scope [55]

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[56].

2. [57]This Regulation applies to the processing of personal data of data subjects residing in the Union[58] by a controller not established in the Union[59], where the processing activities are related to:

   (a) the offering of goods or services,[60] irrespective of whether a payment of the data subject is required[61], 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[62] [63].

---

55 AT scrutiny reservation.

56 FR accepted this criterion. DE and LV expressed some doubt as to its practicability with regard to corporations in the EU that are active on a worldwide basis. Some delegations thought the criterion of establishment should be better defined (PT), e.g. whether it also applied to natural persons (LV).

57 COM stated that this territorial scope stemmed from a human rights obligation to protect EU data subjects also regarding their personal data processed outside the European Union, whose data are processed by a controller not established in the EU.

58 UK remarked that this criterion/condition implied a different data protection regime for the EU establishments of non-EU companies according to whether their customers are EU residents or not. COM indicated it would reflect on this. NO thought the Regulation should also cover the processing done outside the Union by processors established within the Union. At the request of FR, COM clarified that this criterion was intended to apply solely to persons with a residence in the EU, not to persons travelling in the EU.

59 DE, supported by BE, queried whether this would also apply to foreign public authorities (e.g. US DHS) and to endowments or other non-profit associations. The UK, supported by other delegations, pointed to enforceability problems, especially in cases where companies have not appointed a representative in the EU. COM replied that the Charter made no distinction according that 'nature' of the controller and that possible practical enforcement problems should not deter the EU from laying down clear rules on the rights.

60 The Presidency has endeavoured to further clarify this in recital 20.

61 Suggested text to allay concerns expressed by DE and PT, that it needed to be clarified that this also covered services offered free of charge.

62 BE, IE, LT, NO, SE and SK scrutiny reservation.. Several delegations (IE, LT, NO SK and SE) had remarked that more clarity was required as to the exact scope of this, pointing out that 'monitoring' encompassed much more than tracking on the internet. COM replied that Recital 21 offered some clarifications.

63 FR and CZ thought the two subparagraphs should be deleted. FR supported the proposed first sentence of the current paragraph 2, whereas CZ thought one should revert to Article 4(1) (c) of the 1995 Directive. UK would like to see Article 3(2) removed in its entirety.

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[64].

Article 4

***Definitions*[65]**

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (…)[66], in particular by reference to a name[67], an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[68].

(2) (…) [69];

64 BE and UK scrutiny reservation: unclear in which cases this article will apply. Cf. Recital 22.

65 AT scrutiny reservation. AT supports in principle the wider scope of the definitions in the light of future developments. If restrictions should be necessary, they could be added elsewhere (e.g. in connection with the legal consequences like obligations of the data controller).

66 The terms ' by means reasonably likely to be used by the controller or by any other natural or legal person ' have been deleted as FR, LU and UK thought that this concept was too broad. UK thought that the principles of data protection should apply only where a person can be easily identified and not where there is only a remote chance of identification. See new language in recital 23.

67 SE proposal.

68 LU scrutiny reservation: this extended scope lacks legal certainty and takes no account of the intended purpose, context, circumstances or likely privacy impact of processing the personal data concerned. It has not been sufficiently demonstrated that the existing definition of 'personal data' in article 2(a) of Directive 95/46 needs to be replaced. UK thought it was preferable to list these examples in an exemplary manner in a recital rather than in the operative body of the text. FR and UK thought the definition of personal data rather than of data subject should be determining.

69 DE, EE, FR and IT thought that the definition of personal data was no longer compatible with the digitalised age in which even satellite images could fall under this definition. AT however thought that so-called geo data could be the subject of specific sectoral rules. FR and HU proposed to clarify, as is the case under the 1995 Directive, that the data concern an identified or identifiable data subject. DE, ES, LU, SE and SK queried why anonymisation and/or pseudonymisation techniques were not covered and defined here: anonymised data should not be covered by the Regulation. COM referred to Recital 23 which excluded truly anonymised data from the scope of the Regulation. SK also thinks greater clarity is required, also in distinguishing the terms 'personal data' and 'information'.

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

(3) 'processing' means any[70] operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage[71], adaptation or alteration, retrieval, consultation, use, disclosure[72] by transmission, dissemination or otherwise making available, alignment or combination, or erasure[73] [74];

(3a) **'restriction of processing' means limiting the processing of personal data to their storage**;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis[75];

---

70 BE and FR scrutiny reservation: FR thought that this concept was too broad in view of the wide variety of data processing operations possibly covered by this. Read in conjunction with Article 28, this definition would increase rather than reduce administrative burdens on companies. BE thought that the rules applicable to set of operation should more stringent than those for 'any operation'.

71 CY queried what was the difference between 'storage' and 'retention' of data.

72 SK thought the list should also include 'making public' and 'copying'. These two concepts appear to be already covered by the proposed definition. DE also thought further defining might be necessary.

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

74 DE and FR were of the opinion that a separate definition of 'publication of personal data' was required.

75 DE, FR SI, SK and UK scrutiny reservation. UK thought that the concept of 'specific criteria' needed to be clarified. DE and SI thought this was completely outdated concept. COM explained that the definition had been taken over from Directive 95/46/EC and is related to the technical neutrality of the Regulation, as expressed in Article 2(1). DE also thought a recital should clarify the cases covered by this, e.g. in the context of social networks.

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions[76] and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law[77];

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[78] [79];

(7) 'recipient' means a natural or legal person, public authority, agency or any other body[80] to which the personal data are disclosed[81] [; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients];

---

76 UK suggests deleting the reference to the conditions, as this is normally for the processor to determine, not for the controller. UK suggests reverting to the formulation under the 1995 Directive.

77 DE scrutiny reservation on paragraphs 3 to 5: the practical applicability of these definitions in the context of new health services such as Google-health.

78 CZ reservation: CZ wants to delete this definition as it considers the distinction between controller and processor as artificial.

79 SI scrutiny reservation on paragraphs (5) and (6) as data subjects entering data on social media may also fulfil some functions of controller and processor.

80 HU proposed adding 'other than the data subject, the data controller or the data processor'.

81 DE, FR, SI and SE regretted the deletion from the 1995 Data Protection Directive of the reference to third party disclosure and pleaded in favour of its reinstatement. COM argued that this reference was superfluous and that its deletion did not make a substantial difference. FR and UK also pleaded in favour of the reinstatement of the phrase: 'authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients'.

(8) 'the data subject's consent' means any freely given, specific, informed and explicit[82] indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action[83], signifies agreement to personal data relating to them being processed[84];

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or [85]access to, personal data transmitted, stored or otherwise processed[86];

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual which have been inherited or acquired during early prenatal development as they result from an analysis of a biological sample from the individual in question, (…)[87];

---

82 AT, BE, CZ, CY, IE, FR, FI, LT, LU SE, SI, SK and UK scrutiny reservation. Many of these delegations criticised the additional requirements to consent as unrealistic and queried its added value. LU wondered whether 'explicit' consent by the EU legislator would rather protect the controller more when cases were brought to court and where consent would meet all the legal requirements, rather than protecting the data subject. In the same vein, IE wondered whether the proposed requirements would in reality not lead to 'click fatigue'. DE stated that the conditions for electronic consent should be set out here. UK thought that there needs to be consistency with other pieces to legislation such as the E-Privacy Directive. CZ proposed to replace the word 'explicit' by 'provable'.COM argued that this definition merely clarified the 1995 Directive concept of consent, which does not allow for silent or implicit consent. COM referred to recital 25 for clarifying that consent should not be unnecessarily disruptive to the use of the service for which it is provided. See also UK suggestions for amending that recital in the footnote thereto. FR also referred to the need to reflect on consent given by the representative of the data subject.

83 HU suggests adding 'made in writing or by any other recorded means'.

84 DE rejected a 'one-size-fits-all' solution. FR queried why this also covered the representative of the person concerned.

85 ES proposed adding the word 'illegal'; this seems however to be covered by the term 'unauthorised'.

86 COM explained that it sought to have a similar rule as in the E-Privacy Directive, which should be extended to all types of data processing. LU supports having the same rules. DE questioned the very broad scope of the duty of notifying data breaches, which so far under German law was limited to sensitive cases. NL, LV and PT concurred with DE and thought this could lead to over-notification. On the other hand HU and SK preferred a broader definition that covers each and every incidents stemming from the breach of the provisions of the regulation. HU therefore suggests amending the definition as follows '…a breach of (…) the provisions of this regulation leading to any unlawful operation or set of operations performed upon personal data such as ….'. CZ also proposed to refer to a 'security breach' rather than a 'personal data breach'.

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

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which contributes to (…) unique identification of that individual[88], such as facial images, or dactyloscopic data[89];

(12) 'data concerning health' means such information related to the physical or mental health of an individual, which reveal information about **(…)** health **status or** treatments **(…)** of an[90] individual[91];

(12a) 'profiling' means **any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to a natural person, in particular the analysis and prediction of aspects concerning performance at work, economic situation, health,** personal preferences, **or interests, reliability or behaviour, location or movements**;

(13) 'main establishment' means

- as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, **(…)** the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place[92];.

- as regards the processor, the place of its central administration in the European Union, and, if it has no central administration in the European Union, the place where the main processing activities take place;

---

88 FR scrutiny reservation. CZ proposal to replace this wording by '…and individual which are unique for each individual specifically…'

89 SI did not understand why genetic data were not included in the definition of biometric data. AT scrutiny reservation. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. DE thought that the signature of the data subject should be exempted from the definition. CH is of the opinion that the term 'biometric data' is too broadly defined.

90 CZ proposal. RO reservation on the term 'significant'.

91 CZ, DE, EE, FR and SI expressed their surprise regarding the breadth of this definition. AT, BE, SI and LT scrutiny reservation. Proposal to allay the concerns raised. COM scrutiny reservation.

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

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, **represents** the controller, with regard to the obligations of the controller under this Regulation **and may be addressed, in addition to or instead of the controller, by the supervisory authorities for the purposes of ensuring compliance with this Regulation** [93];

(15) 'enterprise' means any **natural or legal person** engaged in an[94] economic activity, irrespective of its legal form, **(…)** including **(…)** partnerships or associations regularly[95] engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings[96];

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

(18) [‘child’ means any person below the age of 18 years;]

(19) 'supervisory authority' means a[97] public authority which is established by a Member State **pursuant to** Article 46;

(…)[98];

(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[99] [100] [101].

---

93 SK scrutiny reservation: unclear whether this definition is linked to Article 25.

94 DE proposed to add the requirement 'independent'.

95 SE criticised the term 'regularly'. It was also queried why the term 'enterprise' was used here, whereas subparagraph 16 used the term 'undertaking' (as in competition law).

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

97 FR proposal, supported by SI, to add 'independent'.

98 The Presidency proposes not to have any definition of third party as a third party will in principle also be a controller.

99 OJ L 204, 21.7.1998, p. 37–48.

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

101 BE, FR and RO suggest adding a definition of ‘transfer’ ('communication or availability of the data to one or several recipients'). RO suggests adding 'transfers of personal data to third countries or international

CHAPTER II

PRINCIPLES

Article 5

Principles relating to personal data processing[102]

Personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject[103];

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[104]; further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83[105];

(c) adequate, relevant, and limited to the minimum necessary[106] in relation to the purposes for which they are processed **(…)**[107];

---

organizations is a transmission of personal data object of processing or designated to be processed after transfer which ensure an adequate level of protection, whereas the adequacy of the level of protection afforded by a third country or international organization must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations'.

102 AT scrutiny reservation. UK thought that the transparency principle should be safeguarded in the relevant sections of the regulation rather than as an overarching principle.

103 At the request of CY and SI, COM clarified that the transparency principle concerns data processing in relation to data subjects and is further detailed in particular by the information requirements (Articles 11 and 14) At the request of DE and SE, COM stated that Member States would still be able to adopt/maintain data protection rules under national law within the limits of the Regulation, where provisions of the Regulation refer to national law.

104 NL and FI pointed out that too strict rules on processing for other purposes could lead to new data collections for already collected data.

105 Based on BE and UK suggestion. RO scrutiny reservation on the placement of this new text.

106 UK suggests replacing 'limited to the minimum necessary' by the terms 'not excessive' (from the 1995 Directive) as it is not always possible to know at the point of collection what the 'minimum necessary' constitutes.

107 Further to FR suggestion, the second part of the sentence was included in the revised recital 23.

(d) accurate and, where necessary[108], 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[109];

(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[110]; personal data may be stored for longer periods insofar as the data will be processed (…)[111] for historical, statistical or scientific (…)[112] purposes[113] **pursuant to** Article 83 (…)[114];

(ee) processed in a manner that ensures appropriate security of the personal data and confidentiality of the processing;

(f) processed under the responsibility (…)[115] of the controller **(…)**[116].

---

108 Further to the remarks from CZ, DE, FR, RO, SE and UK the words 'where necessary' from the 1995 Directive have been reinstated. COM replied that it had been deleted because of divergent Member State practice, but that the updating duty was only required in reasonable cases.

109 CZ suggestion to add 'personal data established as inaccurate shall not be disclosed unless rectified or marked appropriately'. UK pointed out that the duty to erase only arises once the inaccuracy of the data has been established.

110 FR wishes to reinstate the terms 'or further processed' from the 1995 Directive.

111 UK suggestion to delete the word 'solely' so as to allow for data processing for mixed purposes.

112 Suggestion to delete the word 'research' so as to clarify that also storing of data for historical, statistical or scientific purposes which do not amount to research is possible. This concern was raised by SE and NO.

113 Several delegations (DE, NO, SE and SI) requested clarification as to what would be allowed under this purpose. COM referred to recital 126. FR thought the drafting should be better aligned with that of paragraph b).

114 FR, LT, LV, NO and UK scrutiny reservation: these delegations were concerned about the disproportionate administrative burdens ensuing from such periodic reviews

115 Deleted further to the ES and UK remark that liability is not a condition for data processing, but a consequence thereof.

116 BE, LU, NO and FR thought turning the existing means obligation into a result obligation was too onerous and not realistic. As this also overlapped with Article 22 (1), the Presidency suggests deleting the latter part of ths sentence here and set out the obligations on the controller in Article 22.

Article 6

Lawfulness of processing[117]

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

   (a) the data subject has given consent to the processing of their personal data for one or more specific purposes[118];

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

   (c) processing is necessary for compliance with a legal obligation to which the controller is subject[119];

   (d) processing is necessary in order to protect the vital interests[120] of the data subject;

   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[121] [122];

---

117 AT and SK scrutiny reservation.

118 DE and SK asked for an explanation as to the addition of 'for one or more specific purposes'. COM referred to Article 8(2) of the Charter. UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

119 CH and ES queried the relationship to (e) and HU thought that this subparagraph could be merged with 6(1)(e). BE, CZ and LV were of the opinion that other grounds might be used for data processing in the public sector.

120 It may be clarified in a recital that this includes loss or damage to property.

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

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

(f) processing is necessary for the purposes of the legitimate interests[123] pursued by [124]**[the controller or by a controller to which the data are disclosed]** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[125][126]. **This subparagraph** shall not apply to processing carried out by public authorities in the **exercise of their public duties**.[127] [128]

2. (…)

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

(a) Union law, or

(b) the law of the Member State[129] to which the controller is subject.

The purpose of the processing shall be determined in this legal basis. Within the limits of this Regulation, the controller, processing operations and processing procedures, including measures to ensure lawful and fair processing, may be specified in this legal basis.

---

123 FR and LT scrutiny reservation.

124 In accordance with remarks made by CZ, DE, NL, SE and UK, the Presidency suggests to reinstate the words 'or by a third party' from the 1995 Directive. HU could accept it. COM thought that the use of the concept '***a*** controller' should allow covering most cases of a third party.

125 DE asked whether this would allow an absolute prohibition of processing of children's personal data.

126 Link with Article 8 to be clarified**.**

127 BE, PT and UK had suggested deleting the last sentence.

128 The scope of this provision needs to be clarified in a recital.

129 UK scrutiny reservation related to the compatibility of this concept with common law.

4. Where the purpose of further processing is incompatible[130] with the one for which the personal data have been collected, the **further** processing must have a legal basis at least in one of the grounds referred to in points (a)[131] to (e) of paragraph 1[132] [133].

5. (…)[134].

Article 7

Conditions for consent

1. **Where Article 6(1)(a) applies** the controller **shall be able to demonstrate** that consent was provided **by the data subject** .[135] [136].

2. If the data subject's consent is to be given in the context of a written[137] declaration which also concerns another matter[138], the requirement to give consent must be presented in a manner which is clearly[139] distinguishable in its appearance from this other matter.

---

130 Inserted to make the text compatible with Article 5(b). LT thought this required further clarification.

131 AT thought that there should be no reference to (1) (b) as the contract itself would be the ground for data processing if its terms allowed for a change of purpose of data processing.

132 ES and LU though it need further clarification which were non-compatible purposes. COM replied that it wanted to improve the situation under the 1995 Directive, which leads to legal uncertainty. DE and PT reservation: they disagreed with this COM explanation. DE, supported by SE and SI, thought that an exception was needed for publicly available data, e.g. in the context of social networks. To that end it would be preferable if a reference to paragraph 1(f) were also to be included here. PRES indicted that this should be clarified in the text. NO thought that the applicability of the right to information under Article 11 should be explicitly mentioned. UK suggested adding that 'processing necessary for historical, statistical, scientific purposes shall always be deemed compatible processing, provided it is conduced with the rules and condition laid down in Article 83'.

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

134 Deleted in view of reservation by BE, DE, EE, ES, FI, FR, IE, LT, LU, NO, NL, PT, PL, RO, SI, SE and UK.

135 LU, NL and UK thought this proposed rules put a heavy regulatory burden on companies. LU wondered about the compatibility with data retention period obligations, with the principle of data minimisation, and with the obligation for a controller to prove that informed consent was given. DE remarked that one would always need to retain some data for logging purposes. SE requested a clarification (e.g. through a recital) that this did not apply in criminal proceedings.

136 COM has confirmed that this was consent as referred to in Article 6(1)(a) and not consent in the context of a contract (Article 6(1)(b)), to which DE remarked that the data subject might be less protected under contractual law.

137 DE suggested adding 'electronic'.

138 AT asks for a clarification what is meant by 'another matter' (e.g. another purpose for the processing of persona data) and asks whether it would not be necessary to consent separately to this new purpose?'

139 As suggested by ES.

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 (…)[140].

4. **(…)** [141].

[140] BE suggests inserting a provision reading: 'The controller has to fulfil the data subject's request within a reasonable time period'. CZ, LU and SE also thought further clarification was required. AT asked whether the right to deletion would also apply to the results of the processing of the data and to all data of the data subject. It also thought that the format of the withdrawal should be further clarified (the same as for the consent, i.e. written declaration?).

[141] Deleted in view of scrutiny reservations by BE, CZ, DE, EE HU, IE, LT, SE, SI and PL. SI referred to the case of asylum seekers whose data were processed in SI on the basis of their consent. COM indicated that this would be excluded by the Data Protection Regulation as such processing does not rely on a freely given consent and should be based on a statutory basis.. DE, IE and NL had pleaded to reconsider this rule, which it considered to be very broad. DE remarked that the absence of dependence should be considered as part of the requirement of freely given consent. COM reservation on deletion.

Article 8

***Processing of personal data of a child*[142]**

1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child[143], the processing of personal data of a child below the age of 13 years[144] shall only be lawful if and to the extent that consent as referred to in Article 7[145] is given or authorised by the child's parent or **guardian.**[146].

   The controller shall make reasonable efforts to obtain (…)[147] consent, taking into consideration available technology[148].

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[149].

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(…)[150].

---

142 AT and SE scrutiny reservation. CZ and UK reservation: CZ and UK would prefer to see this Article deleted. NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child.

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

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

145 It should be clarified that this applies only if consent is the ground for data processing. DE, supported by NO, opined it could have been integrated into Article 7.

146 IT asked how minors could be represented. FR queried whether this implied that for all other rights minors needed to be represented by their parents/legal guardian.

147 DE suggestion: the burden of proof is regulated in Article 7.

148 PL, PT, SE and UK queried the verifiability of compliance with this obligation. UK therefore suggested deleting the final sentence.

149 DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law.

150 The last part of the provision was deleted as several delegations queried the expediency of (using delegated acts for) setting derogations for SMEs to an obligation aimed at protecting children: CZ, DE, EE, ES, FR, LV, PT and SE. DE thought this should be done through Member State law.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)][151].

Article 9

***Processing of special categories of personal data*[152]**

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or philosphical beliefs[153], trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences[154] or related security measures shall be prohibited.[155]

---

151 LU is not convinced that implementing acts are necessary in this instance. UK suggested deleting paragraphs 3 and 4.

152 AT, PT and LI scrutiny reservation. DE, supported by CZ and UK, criticised on the concept of special categories of data, which does not cover all sensitive data processing operations. CZ pleaded in favour of a concept of risky processing. SK also thought the criterion should be context based and the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. COM referred to the general discussion on an open versus closed list of sensitive data.

153 CY, FR and AT deplored the deletion of the adjective 'philosophical' before 'beliefs', as this made the concept too broad. IE also thought this was too vague. COM referred to the wording used in the Charter. RO pleaded for inserting biometric data.

154 As suggested by FR. EE reservation: this should be left to the Member States. NO, NL and AT reservation: the inclusion of suspicion of criminal offences should be considered. At the request of CY, COM clarified that disciplinary convictions were not covered by the list.FR thought the wording of the 1995 Directive should be copied. LT suggested to add, following 'security measures', the following text: 'or any other kind of data which enable disclosure of personal data indicated in this paragraph'

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

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

(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject[156]; or

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards[157]; 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[158]; or

(e) the processing relates to personal data which are manifestly made public[159] by the data subject; or

---

156 DE questioned whether one needed consent as a specific basis here, referring also to the complicated interaction between Member State and EU law. FR scrutiny reservation. LU thinks that special categories of data and 'normal' data should not be put on the same footing.

157 DE queried whether this paragraph obliged Member States to adopt specific laws on data protection regarding labour law relations; COM assured that the paragraph merely referred to a possibility to do so. COM also stated that labour relations were as a rule based on a contract and therefore the conditions laid down in Article 7 (4) would not apply here.

158 HU thinks this subparagraph can be deleted as it overlaps with (a).

159 DE, IE SE and SI raised questions regarding the exact interpretation of the concept of manifestly made public (e.g. whether this also encompassed data implicitly made public and whether the test was an objective or a subjective one). In view of the increased importance of such data (inter alia via social networks), the

(f) processing is necessary for the establishment, exercise or defence of legal claims in court proceedings or otherwise[160]; or

(g) processing is necessary for the performance of a task carried out **for reasons of** substantial[161] public interest, on the basis of Union law, or Member State law which shall provide for suitable measures[162] to safeguard the data subject's legitimate interests; or

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81[163]; or

(i) processing is necessary for historical, statistical or scientific (…)[164] purposes[165] subject to the conditions and safeguards referred to in Article 83; or

---

suggestion was made to draft a separate article on the handling of such data, covering both sensitive and non-sensitive data.

160 ES suggests adding 'of any kind'. LT requests the deletion of 'or otherwise'.

161 Addition suggested by AT, DE and SE, as this was the exact term from the 1995 Directive. UK reservation on this reinsertion.

162 CY queried whether this was the same as 'adequate safeguards'.

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

164 Suggestion to delete the word 'research' so as to clarify that also storing of data for historical, statistical or scientific purposes which do not amount to research is possible. This concern was raised by SE and NO.

165 ES suggests adding: 'or for preliminary official or administrative investigation to determine biological parentage'.

(j) processing of data relating to criminal convictions and offences[166] or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards[167]. (…)[168].

3. (…)[169].

Article 10

Processing not requiring identification

If the purposes for which a controller processes **personal** data do not require the identification of a data subject **by the controller,** the controller shall not be obliged to acquire **(…)** additional information in order to identify the data subject for the sole purpose of complying with (…) this Regulation.[170] [171].

166 UK, supported by NL and PL suggested adding 'criminal offences' (cf. 1995 Directive). EE was opposed to this as under its constitution all criminal convictions were mandatorily public.

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

168 ES thought that the last sentence did not belong in this Regulation.

169 Deleted in view of the reservations by BE, CZ, DE, ES, IE, LU, PT, SE, SI, SK and UK.

170 AT, DE, ES, FR, HU and UK scrutiny reservation. FR and ES had a preference for the modified paragraph 1. UK and IE thought this should be clarified in recitals. Several delegations highlighted the need for devising clear rules on anonymous data and spelling out the conditions under which these are not subject to (some of) the rules of this Regulation. See revised recital 23.

171 BE proposed adding a second paragraph 'The processing of data which allows individualising a data subject without identifying him is not subject to Articles 15 to 19 and Article 32'. HU indicated that in case where 'the data processed by a controller do not permit the controller to identify a natural person', such processing cannot be qualified as personal data processing. Therefore the person processing such 'impersonal data' cannot be deemed a 'controller'. For HU the question arises whether such a provision is necessary or whether it is obvious that processors of data relating to unidentifiable natural persons shall not have the obligations and rights of a 'controller'.

CHAPTER III
RIGHTS OF THE DATA SUBJECT[172]

SECTION 1

TRANSPARENCY AND MODALITIES

Article 11
Transparent information and communication

1. (…)

2. (…)[173].

Article 12
Transparent information, communication and modalities for exercising the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Article 14, 14 a and 20(4) and any communication under Articles 15 to 19 and 32[174] relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language, (…)[175] in particular where addressed specifically to a child. The information shall be provided in writing[176], or where appropriate, electronically or by other means[177].

---

172 General scrutiny reservation by UK on the articles in this Chapter. DE remarked the title might need to be adapted as this chapter also contains obligations for data processors. IT is of the opinion that the chapter appears to be lacking any systematic structure: before laying down provisions on the mechanism for exercising rights (currently contained in Article 12), it would be better if the provisions on information (currently in Article 14) were inserted after Article 11, followed by the articles on the rights of the data subject (currently Articles 15 to 19) and then the rights in relation to recipients (currently Article 13) and, lastly, in view of its purely procedural nature, the mechanism for the exercise of those rights.

173 Moved to Article 12 (1).

174 Suggestions so as to clarify that the obligation is a means obligations (cf. FR and ES proposal) and is restricted to the obligations referred to. This is also intended to reduce the risk of litigation regarding compliance with an essentially subjective test of 'an intelligible form, using clear and plain language, adapted to the data subject' (cf. UK, DE and NL). DE remarked that the exact scope of this article needs to be clarified and in particular in which case there is an duty on the data processor to actively provide information and in which case this may happen on request from the data subject.

175 The requirement 'adapted to the data subject' was deleted as this is clearly both too onerous and to vague to be applied in practice (cf. IE, SE and UK).

176 DE thought this should be limited to informing the data subject that the obligations referred to in the beginning of this paragraph had been complied with. It queried why the information could not be provided orally. COM (supported by IT) replied that it was important to have written trace of the reply.

177 FR and BE proposal. Recital 46 was modified in order to clarify that this may be done through a website.

1a[178]. The controller shall facilitate **the processing of**[179] data subject requests under Articles 15 to 19 (…)[180]. **(…)**[181].

2. The controller shall provide the information referred to in Article 15 and 20(4) and information on action taken on a request under Articles 16 to 19[182] to the data subject without undue delay and at the latest within one month of receipt of the request[183] (…). This period may be extended for a further two months when necessary[184], taking into account the complexity of the request and the number of requests[185]. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.

3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action[186] and on the possibility of lodging a complaint to a supervisory authority (…)[187].

---

178 Former paragraph 2 of Article 11 moved here, as it seems more appropriate to put this requirement after the one to have procedures in place. SI and UK thought this paragraph should be deleted.

179 NL proposal.

180 This sentence was deleted at the suggestion of DE, as the concept of 'mechanisms for facilitating' was very vague and not appropriate for a legally binding text.

181 Moved to recital 47.

182 Suggestions so as to clarify that the obligation is a means obligations (cf. FR and ES proposal) and is restricted to the obligations referred to. This is also intended to reduce the risk of litigation regarding compliance with an essentially subjective test of 'an intelligible form, using clear and plain language, adapted to the data subject' (cf. UK, DE and NL). DE remarked that the exact scope of this article needs to be clarified and in particular in which case there is an duty on the data processor to actively provide information and in which case this may happen on request from the data subject.

183 IE, UK and SE pleaded in favour of deleting the one-month period. BG, PT, and SE thought it more simple to revert to the requirement of 'without excessive delay' under the 1995 Data Protection Directive. BE pleaded in favour of two months. The Presidency proposes to keep the one-month period but to extend the exceptional period to two months.

184 Several delegations (DE, ES, FR, HU, IE and LT) stated that it was unclear in which cases one - now two - extra month(s) would apply. DE, BE and AT thought there might be other grounds which would justify a prolongation of the period within one month. IE thought it more simple to delete those cases and revert to the requirement of 'without excessive delay' under the 1995 Data Protection Directive.

185 The reference to several data subjects exercising their rights was deleted: cf. those delegations (FR and HU), which thought this requirement was unclear.

186 SK thought the reasons should be clearly defined lest controllers abuse the possibility to refuse.

187 The reference to 'seeking a judicial remedy' was deleted. IE, NL, SI and UK pointed out that this is too detailed, especially as any meaningful implementation of it would imply that the details of the judicial authority competent in that specific case would need to be provided. The fact that the possibility of a judicial remedy is not mandatorily communicated to the data subject does not constitute a violation of the constitutional rights that exist. Also the reference to the time period deleted. UK thought the whole reference to complaints should be deleted.

4. Information provided under Articles 14, 14a and 20(4) and any communication under Articles 15 to 19 and 32[188] shall be provided free of charge[189]. Where requests from a data subject are (…)[190] unfounded or manifestly excessive, in particular because of their repetitive character[191], the controller (…) may decline the request[192]. In that case, the controller shall bear the burden of demonstrating the unfounded or manifestly excessive character of the request.[193]

4a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject[194].

5. (…)

6. (…)

---

188 This cross-reference was unclear and was replaced by a reference to the Articles concerned.

189 In the context of Article 15, CZ, DE, IE, LV and UK argued that controllers should be allowed to charge a nominal fee.

190 BE, LT and PL thought the criterion of 'manifestly excessive' required further clarification, e.g. through an additional recital. NL proposed to replace it by 'a manifestly abuse of right'. It is hoped that the Swedish suggestion to refer to excessive requests will obviate the need for further clarification. COM reservation on deletion.

191 It was also argued that this not contrary to human rights requirements. NL and PL opined that also the interests of the controller should be taken into account. BE, LT and PL thought the criterion of 'manifestly excessive' required further clarification, e.g. through an additional recital. NL proposed to replace it by 'a manifestly abuse of right'. The Swedish suggestion to refer to excessive requests will obviate the need for further clarification.

192 SK thought there was a need to define more clearly in which cases the controller could refuse. AT thought the text should specify that the fee must be proportionate. NL and PL opined that also the interests of the controller should be taken into account. Several delegations (IE, LT, NL, SK and UK) emphasised the need of having a filtering mechanism in place against speculative requests, e.g. through a nominal fee.

193 DE pointed out that this was a basic principle of burden of proof, which should not be mentioned.

194 Suggestion further to the remarks by SI, AT, RO and DE that there was a need for an obligation on the part of the controller to verify the identity of the data subject before granting access to its personal data (cf. Article 31 of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (= Prüm decision). DE also referred to recital 52, which stresses the importance of verifying the identity of the requestor.

Article 13

Rights in relation to recipients

(...)[195]

SECTION 2

INFORMATION AND ACCESS TO DATA

Article 14

Information <u>to be provided where the data are collected from the data subject</u>[196]

1. Where personal data relating to a data subject are collected <u>from the data subject</u>, the controller shall (…), <u>at the time when personal data are obtained</u>, provide the data subject with the following information:

   (a) the identity and the contact details of the controller and, if any, of the controller's representative<u>; the controller may</u>[197] <u>also include the contact details</u> of the data protection officer<u>, if any</u>;

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

---

195 This Article was moved to Article 17b.

196 Several delegations, while agreeing with the principle as such, thought that this provision was too detailed: CZ, DE, EE, ES, LU, MT, NL, SE, SI, PT and UK. DE and NL argued that also here a more risk-based approach should be taken by differentiating between low-risk and high-risk processing operations. DE, supported by ES and NL, asked the Commission to provide an assessment of the extra costs for the industry under this provision. DE and IE thought that this article should distinguish between data which need to be communicated to the data subject and other data which need to be available to the data subject. Having regard to the many comments by delegations that the right to information should distinguish according to whether or not the personal data were collected from the data subject, Article 14 was split into two separate articles.

197 Made optional further to the remarks by CZ, DE, ES, NL and UK.

1a. In addition to the information referred to in paragraph 1, the controller shall[198] provide the data subject with any further information necessary to ensure fair and transparent processing **in respect of the data subject** [199], having regard to the specific circumstances in which the personal data are processed, such as:

(a) the envisaged period for which the personal data will be stored[200];

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;

(c) the recipients or categories of recipients of the personal data[201];

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

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data, including for direct marketing purposes[202];

(f) the right to lodge a complaint to a supervisory authority (…)[203];

(…)

(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data[204].

---

198 DE, EE, and PL asked to insert "on request".

199 Inspired by Article 10 of the 1995 Data Protection Directive.

200 CZ, EE, ES, IE, IT, LU, MT, SE, SI and UK thought that this should not be mentioned.

201 AT, DE and NL thought that this concept was too vague (does it e.g. encompass employees of the data controller). Regarding online data anyone could be a recipient and some cases of recipients were evident

202 FR questioned whether it was necessary to single out this sector.

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

204 CZ, DE, ES and NL reservation. NL pointed out that these general contract terms would already be communicated to the data subject and at any rate in case of standard contracts were often not read.

2. (…)

3. (…)

4. (…)

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

6. (…)

7. (…)

8. (…)

Article 14 a

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

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

   (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may[205] also include the contact details of the data protection officer, if any;

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

[205] Made optional further to the remarks by CZ, DE, ES, NL and UK.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with any further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed, such as:

(a) the categories of personal data concerned;

(b) the envisaged period for which the personal data will be stored;

(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;

(d) the recipients or categories of recipients of the personal data;

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data**, including for direct marketing purposes**;

(f) the right to lodge a complaint to a supervisory authority (…);

(g) the origin of the personal data[206], unless the data originate from publicly accessible sources[207].

3. The controller shall provide the information referred to in paragraphs 1 and 2[208]:

(a) (…) within a reasonable period[209] after obtaining the data, having regard to the specific circumstances in which the data are processed, or

(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

---

206 BE indicated that the exact source should be provided only upon request of the data subject, under Article 15(1)(g). This should also be clarified in a recital. COM reservation on such exception.

207 DE, FR, FI, SI and UK pleaded for an exception for publically available data. AT scrutiny reservation.

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

209 FR and SK thought the reference to a reasonable period should be deleted because of its vagueness. DE proposed to strengthen it.

4. Paragraphs 1 to 3 shall not apply where and insofar as:

(a) the data subject already has the information[210]; or

(b) the provision of such information in particular when processing personal data for historical, statistical or scientific purposes[211] proves impossible or would involve a disproportionate effort[212]. In such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[213], for example by using pseudonymous data[214]; or

(c) obtaining or disclosure is expressly laid down by Union or Member State[215] law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the data originate from publicly available sources[216]; or

(e) where the data must remain confidential in accordance with a legal provision or on account of the overriding **legitimate** interests of a third party[217].

5. (…)

6. (…)

---

210 SK thought it would be preferable to establish the burden of proof on the side of the data controller.

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

212 PL and FR queried what would be the criteria for determining what constitutes a disproportionate effort (the example of Google Street view was cited). DE queried whether the provision of information on creditworthiness of a data subject would be covered by this exemption.

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

214 Further to DE suggestion. The Presidency thinks that a definition of pseudonymised personal data should be added in Article 4 of the Regulation.

215 Further to DE suggestion.

216 DE, FR, FI, SI and UK pleaded for an exception for publically available data. By inserting the exemption here, paragraph 3 is also covered. COM and AT reservation.

217 Further to DE proposal.

Article 15

Right of access for the data subject[218]

1. [219]The data subject shall have the right to obtain from the controller at reasonable intervals[220], on request, confirmation as to whether or not personal data concerning him or her are being processed. Where such personal data are being processed, the controller shall **communicate** the personal data undergoing processing and the following information to the data subject:

   (a) the purposes of the processing;

   (b) (…)

   (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries[221];

   (d) the envisaged[222] period for which the personal data will be stored;

   (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

   (f) the right to lodge a complaint to a supervisory authority (…)[223] [224];

---

218 DE, NL and SE scrutiny reservation. DE, LU and UK expressed concerns on overlaps between Articles 14 and 15. FR, IE, LU and PL thought that it needed to be clarified that the data subject's identity can be verified; however this has now been clarified in Article 12 (2). ES stressed that the right to access would need to be modulated further and to that end recital 51 was modified. LU also queried how the obligations under this article related to the rule, expressed in recital 52, that a controller should not retain data for the unique purpose of being able to react to potential requests.

219 DE proposed to subject this right to the second sentence of paragraph 4 of Article 12.

220 Proposal of NL, IE, DK, SE, FI, and UK inspired by Article 12, (a) of the 1995 Directive.

221 Delegations made different suggestions in order to encapsulate the ECJ case law (*Rijkeboer*, C-553/07, OJ C64 of 08.03.2008): BE suggested adding 'as long as the data subject has the right of access'; IT suggested specifying 'third party recipients of the data'.

222 ES proposed adding "where possible"; FR empahasisd the need of providing an exception to archives.

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

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

(g) where the personal data are not collected from the data subject[225], any available information as to their source[226];

(h) in the case of **decisions** referred to in Article 20, knowledge of the logic involved in any automated data processing[227]**as well as** the significance and envisaged consequences of such processing[228].

2. (…)[229]**Where personal data are processed by electronic means and in a structured and commonly used format, the controller shall provide a copy of the data in that format to the data subject[230].**

3. (…)

4. (…)

5. [The rights provided for in Article 15 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met][231].

---

225 DE proposal.

226 PL and SK scrutiny reservation: subparagraph (g) should be clarified.

227 Text addition at the proposal of BE, NL and PL, inspired by Article 12, (a), 3rd indent of the 1995 Directive.

228 DE thought this should be made more concrete. CZ and FR likewise harboured doubts on its exact scope.

229 This paragraph was deleted. BE, CH, CZ, DE, ES and UK could not see how the first sentence differs from the obligation under paragraph 1(g).

230 The Presidency has moved this text from Article 18(1).

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

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[232]

1. (…) The data subject shall have the right[233] to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed,[234] the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…)[235] statement[236].

2. [The rights provided for in Article 16 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.][237]

---

232 DE and NL scrutiny reservation. UK and DE thought the risk-based approach should also be implemented regarding this article by introducing proportionality in this article. DE asked why there was no possibility of blocking data in case the accuracy of the data cannot be verified. This appears, however, to be regulated in Article 19. DE also thinks that the right to rectification must be replaced by the right of reply if the personal data are processed on a commercial basis, are from generally accessible sources and are stored for documentation purposes, for example press evaluation databases which would themselves become inaccurate following rectification. The data may be transferred only together with the reply. Data referred to in Article 9 should, however, also be rectified in such cases.

233 UK suggested to insert the qualification ' where reasonably practicable' UK also suggested inserting the qualification 'where necessary'. NL and PL had suggested providing an exception where 'the exercise of the right to rectification proves impossible or would involve a disproportionate effort' (cf. Article 11(2) of the 1995 Data Protection Directive). DE thought there should be no subjective right to correction, but only an objective right

234 Further to UK suggestion.

235 Further to IE suggestion. This change seeks to accommodate, inter alia, the BE remark that data subjects should have the right to supplement subjective assessments.

236 HU, LT, SI and DE scrutiny reservation: DE and SI particularly query the application of the right to completion for the public sector. This problem could potentially be solved in the same manner as in Article 11(2) of the 1995 Data Protection Directive by exempting cases where 'recording or disclosure is expressly laid down by law'. However, this should be examined in the context of the horizontal discussion on the application of the Regulation to the public sector.

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

Article 17

Right to be forgotten and to erasure[238]

1. The (…) controller[239] shall have the obligation to erase personal data **without delay** (…)[240] and the data subject shall have the right to **obtain** the erasure of personal data[241] **without delay** (…) [242] where one of the following grounds applies:

---

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

239 DE pointed to the difficulties in determining who is the controller in respect of data who are copied/made available by other controllers (e.g. a search engine) than the initial controller (e.g. a newspaper). AT opined that the exercise of the right to be forgotten would have take place in a gradual approach, first against the initial controller and subsequently against the 'secondary' controllers. ES referred to the problem of initial controllers that have disappeared and thought that in such cases the right to be forgotten could immediately be exercised against the 'secondary controllers' ES suggested adding in paragraph 2: ' Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof'. The Commission, however, replied that the right to be forgotten could no be exercised against journals for reasons of freedom of expression. According to the Commission, the indexation of personal data by search engines is a processing activity not protected by the freedom of expression.

240 DE and ES remarked that once the controller has erased the data he is unable to further disseminate them and this reference is therefore meaningless.

241 Further to remarks by DE, the chapeau of paragraph 1 has been redrafted so as to clarify that this is an objective duty of the data controller (cf. wording of paragraph 3), regardless of the exercise of the subjective right of the data subject under paragraph 1. FR stressed the right to be forgotten should also be available in relation to personal data made available by third parties

242 Several delegations (BG, CZ, DE, FR, NL, UK) have stated that the reference to children conveys the impression of a different regime for data made available by children (DE moreover pointed to the practical difficulties in determining the applicability of any such special regime).

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

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1)[243] (…)[244] and (…) there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data and **there are no overriding legitimate grounds for the processing pursuant to Article 19(1) or the data subject objects to the processing of personal data pursuant to Article 19(2)**;

(d) **the data have been unlawfully processed**[245];

(e) the data have to be erased for compliance with a legal obligation **to which the controller is subject**[246].

2. (…)[247]

---

243 DE and SK thought that the consequences of any withdrawal or limitation of consent should rather be regulated in Article 7. DK queried why there was no reference to Articles 9 and 20 DE also queried whether any such withdrawal would have an effect *ex tunc* or *ex nunc*. DE, NL and PL queried about the impact of Article 21.

244 The Presidency agrees with DE that Article 7 does not allow limiting consent in time other than by withdrawing it. Should delegations feel there is a need to do so; this should be done in Article 7.

245 Further to the remarks by several delegations (BG, CZ, DE, ES, IE, IT, LV, LU, NL, PT and UK) to the effect that 'other reasons' needed to be specified, the Presidency has deleted the text and replaced it by a reference to unlawful processing.

246 BE proposal. The Presidency would welcome views on whether, and if so how, this Article should apply to the public sector.

247 This paragraph has been moved to paragraph 3a.

3. **Paragraph 1 shall not apply**[248] to the extent that (…) **processing** of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80[249]; [250]

(b) for reasons of public interest in the area of public health in accordance with Article 81[251];

(c) for historical, statistical and scientific (…) purposes in accordance with Article 83;

(d) for compliance with[252] a legal obligation to **process** the personal data by Union or Member State law to which the controller is subject[253](…)[254];

(e) (…)[255];

(f) (…).

---

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

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

250 The Presidency favours removal of the "journalistic purposes" restriction in Article 80 and its replacement with "freedom of expression and information" as referred to in Article 11 of the Charter.

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

252 UK suggested adding 'or to avoid a breach of'.

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

254 Deleted as it was not acceptable to put different conditions to Member State laws than to Union law.

255 The reference to paragraph 4 has been deleted in accordance with the remarks by delegations (DE, PT, UK) to the effect that erasure should be clearly distinguished from restricting the processing of personal data.

3a. Where the controller[256] (…) has made the personal data[257] public[258] **and is obliged pursuant to paragraph 1 to erase the data**, it shall take all reasonable steps[259], including technical measures, in relation to data for the publication of which the controller is responsible, to inform **controllers**[260] which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data[261],

4. **(…)**[262].

5. (…)

256 BE queried whether this also covered controllers (e.g. a search engine) other than the initial controller

257 LU asked whether the limitation in paragraph 1 to personal data 'relating to them' also applies to paragraph 2.

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

259 LU queried why the reference to all reasonable steps had not been inserted in paragraph 1 as well. COM replied that paragraph 1 expressed a results obligation whereas paragraph 2 was only an obligation to use one's best efforts. ES thought the term should rather be 'proportionate steps'. DE, ES and BG questioned the scope of this term. Es queried whether there was a duty on controllers to act proactively with a view to possible exercise of the right to be forgotten.

260 BE, supported by ES and FR, had suggested to refer to 'known' controllers (or third parties).

261 BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (EE, IE, NL, SI) questioned the feasibility of applying this rule to national archives or more generally the expediency of applying it to the public sector (BE and PL). COM indicated national archives would be covered by paragraph 3(c).

262 DE agreed with this rule but thought it should made into a general rule. The Presidency has moved this to paragraph 2a of Article 22 (see 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155).

Article 17*a*

Right to restriction of processing 263

1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:

   (a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[264];

   (b) the controller no longer needs the personal data for the **purposes of the processing**, but they **are required** for the establishment, exercice or defence of legal claims **by the data subject** [265];

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

   (d) (…)[266] [267].

2. (…)[268].

---

263 The former paragraph 4 of Article 17 has been redrafted into a new Article, as the cases listed here are not always alternatives to erasure, as has been pointed out by several delegations (AT, FR, IT and LU).

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

265 BE suggestion, supported by NL and UK.

266 Deleted in accordance with the UK remark that the right to data portability is separately regulated in Article 18 and there is no need to 'import' it here in the right to be forgotten. It has moreover been pointed out by delegations (DE and EE) that there may be cases where the exercise of the right to data portability will not automatically imply that the initial controller may no longer use the data.

267 With reference to Write Once Read Many (WORM)-Systems and paper deeds, DE suggested adding as sub paragraph (e) ' the erasure of the personal data in accordance with Article 17 is impossible or would involve a disproportionate effort due to the special nature of the storage of the data'.

268 Moved to Recital 54a.

3. **Where processing of personal data has been restricted under** paragraph 1, **such** data may, with the exception of storage, only be processed **with the data subject's consent or** for the establishment, exercise or defence of legal claims[269] **by the controller or the processor**, (…) or for the protection of the rights of another natural or legal person or for **reasons of substantial** public interest[270].

4. **The controller shall implement mechanisms to ensure that a periodic review of the need to retain restricted data is performed. Restrictions on the processing shall not be lifted without the consent of the data subject[271].**

5. **(…)**[272].

Article 17b

Notification obligation regarding rectification or erasure [273]

The controller shall communicate any rectification, erasure **or restriction of processing** carried out in accordance with Articles 16, 17 **and 17a**[274] to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort[275].

---

269 BE suggestion, supported by NL and UK.

270 ES asked who was to define the concept of public interest

271 Further to IT proposal. DE, SK and UK thought the conditions for lifting the restriction should be specified here. IE queried how this paragraph was linked to the right to rectification under Article 16. LT thought there should be deadlines to restrictions on processing.

272 DE agreed with this rule but thought it should made into a general rule. UK thought that the requirement for controllers to set up mechanisms for periodic review of the need for storage does not fit in an article primarily about erasure and the right to be forgotten and needed to be moved to Chapter IV on controller's general obligations. The Presidency has accordingly moved this to Article 22a (see 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155).

273 This Article was moved from Article 13 to here, as it refers to the preceding Articles 16 and 17. Whilst several delegations (ES, IT and PL) agreed with this proposed draft and were of the opinion that it added nothing new to the existing obligations under the 1995 Directive, other delegations (DE, SK and NL) pointed to the possibly far-reaching impact in view of the data multiplication since 1995, which made it necessary to clearly specify the exact obligations flowing from this proposed article. Thus, DE was opposed to a general obligation to log all the disclosures to recipients in order to ensure compliance with Article 13, now 17b. DE also pointed out that the obligation should exclude cases where legitimate interests of the data subject would be harmed by a further communication to the recipients, that is not the case if the recipient would for the first time learn negative information about the data subject in which he has no justified interest. Relevant examples should be explained in a recital.

274 DE suggests including successful objections made in accordance with Article 19.

275 BE and ES asked that the concept of a 'disproportionate effort' be clarified in a recital. UK pointed out that in an online environment communication to all recipients may not be possible. SK pointed out that in its legal system a distinction is made between making personal data available and the provision of personal data.

Article 18

Right to data portability[276]

1. (…)[277]

2. Where the data subject has provided personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit these (…) data (…)[278] **where they are** retained by an automated processing system, into another one in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn[279].

2a. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights.

[3. The Commission may specify (…) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

---

276 UK reservation: while it supports the concept of data portability in principle, the UK considers it not within scope of data protection, but in consumer or competition law. Several other delegations (DK, DE, FR, IE, NL, PL and SE) also wondered whether this was not rather a rule of competition law and/or intellectual property law or how it related to these fields of law. Therefore the UK thinks this article should be deleted. Reference was made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK). DE, DK and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, SE and UK pointed to the considerable administrative burdens this article would imply. BE, DE, FR IE, NO, PL; SE and UK failed to see how this right could also be applied in the public sector, to which COM replied that paragraph 2 was implicitly limited to the private sector. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger ongoing research or the continuity of the service. IT and NL stated that the relationship between the right to a copy of personal data and the right to access should be clarified. FR and IE were broadly supportive of this right. SK thought that the article was unenforceable.

277 Moved to Article 15(2).

278 BE and FR, while having no difficulties regarding raw data, were - inter alia for intellectual property - reasons opposed to the application of this right to aggregated/modified data having undergone processing. BE pointed to the difficulties of the direct marketing sector of applying the concept of 'any other information provided by the data subject'

279 HU thought the last part of the phrase need further precision.

4. [The rights provided for in Article 18 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met .][280].

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19
Right to object[281]

1. The data subject shall have the right to object, on reasoned grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point[s] (…) [(e) and] (f) of Article 6(1)[282]. In such cases the personal data shall no longer be processed unless the controller demonstrates (…) legitimate grounds for the processing which override the interests or (…) rights and freedoms of the data subject[283].

---

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

281 DE, ES, EE, NL, AT, SI and SK scrutiny reservation.

282 UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. LU queried why Article 6(1) (c) was not listed here and AT thought Article 6(1) (d) and (e) should be deleted. BE, CZ, DE and HU likewise thought that the reference to Article 6(e) should be deleted.

283 DE and FI queried the need for new criteria, other than those from the 1995 Directive. The need for clarification of the criterion 'compelling legitimate grounds' (DK, FR, LU, PL, SK and UK) and of the right to object in case of direct marketing (recitals 56 and 57, NL) were emphasised. COM stressed that the link with the 'particular situation' was made in order to avoid whimsical objections. IE and NL queried the need to put the burden of proof on the controller regarding the existence of compelling legitimate grounds. CZ also stated that this risked making processing of data an exceptional situation due to the heavy burden of proof. NL and SE queried whether the right would also allow objecting to any processing by third parties.

1a[284]. Where an objection is upheld[285] pursuant to paragraph 1 (…), the controller shall no longer (…)[286] process the personal data concerned except for the establishment, exercise or defence of legal claims[287].

2. Where personal data are processed for direct marketing[288] purposes, the data subject shall have the right to object free of charge at any time[289] to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…)[290] **and** shall be presented clearly and separately from any other information[291] [292].

---

284 Moved from paragraph 3.

285 GR queried what happened pending the resolution of an objection.

286 DK, SE and SK thought 'otherwise' should be deleted, unless COM explained its meaning. BE pointed out that processing covered 'use'. AT asked how this related to the right to erasure. ES proposed to reformulate the last part of this paragraph as follows: 'shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise shall no longer use or otherwise process the personal data concerned'.

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

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

289 IT proposal.

290 Deleted at the suggestion of DE, as this is already covered by paragraph 2 of Article 11, now moved to Article 12, paragraph 1. DE deplored that the possibility existing under Article 14(b) DPD 46/95 to 'be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing ' was no longer mentioned.

291 UK scrutiny reservation. PL queried why the second sentence did not apply to the right to object in all cases. This distinction, however, also exist under Article 14 of the 1995 Directive. NO queried whether the existence of a central register of data subjects objecting to direct marketing, the regular consultation of which was compulsory, was compatible with the proposed paragraph 2. At the request of several delegations (FR, LT), COM confirmed that this paragraph was not meant to create an opt-in system and that the E-Privacy Directive would remain unaffected. SE queried about the consistency of this paragraph, which stated that the right to object was free of charge, with paragraph 4 of Article 12, where this was not the case. DE feels there is a need to clarify the relationship between Article 19(2) on the one hand and Article 6(1)(f) and Article 6(4) on the other. It can be concluded from the right to object that direct marketing without consent is possible on the basis of a weighing of interests. On the other hand, Article 6(1)(f) no longer refers to the interests of third parties and Article 6(4) also no longer refers to Article 6(1)(f) in regard to data processing which changes the original purpose. DE is therefore of the opinion that this also needs to be clarified in view of online advertising and Directive 2002/58/EC and Article 89 of the Proposal for a Regulation.

292 IE, supported by SI, pointed out that the campaigning actions of political parties and individuals seeking election to political office, which are essential features of democratic political systems, must be protected.

2a. **Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed.**

3. (...)

4. [The rights provided for in Article 19 do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met[293]].

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

Article 20

Decisions[294] ***based on profiling***[295]

1. Every data subject[296] shall have the right not to be subject **to a decision based on** profiling[297] **concerning him or her** which produces legal effects (…) or **adversely**[298] **affects**[299] (…) him or her **unless such** processing[300]:

(a) is carried out in the course of the entering into, or performance of, a contract between the data subject and **a** data controller (…) [301] **and** suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right**s of the data subject** to obtain human intervention **on the part of the controller to express his or her point of view and to contest the decision** [302]; or

---

294 BE, IE and SK expressed a preference for the term 'decision' (from the 1995 Directive) over 'measure'.

295 ES, FR and UK reservation. In accordance with the suggestion by NL, supported by ES, FR, LV, PL and PT, the text has been redrafted on the basis of the definition contained in Recommendation RM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). Further to the suggestion by FR the concept of profiling itself ha been defined in Article 4 and Article 20 is now limited to the applicable rules. DE thinks this provision must take account of two aspects, namely, whether and under what conditions a profile (= the linking of data which permits statements to be made about a data subject's personality) may be created and further processed, and, secondly, under what conditions a purely automated measure based on that profile is permissible if the measure is to the particular disadvantage of the data subject. It appears expedient to include two different rules in this regard. According to DE Article 20 only covers the second aspect and DE would like to see a rule included on profiling in regard to procedures for calculating the probability of specific behaviour (cf. Article 28b of the German Federal Data Protection Act, which requires that a scientifically recognized mathematical/statistical procedure be used which is demonstrably essential as regards the probability of the specific behaviour).

296 UK, LU and DE suggestion.

297 DK remarked that this was an open list of profiling measures and that it would prefer a closed list for the sake of legal certainty.

298 DE wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there also cases of automated data processing which actually were aimed at increasing the level of data processing (e.g. in case of children that are automatically excluded from certain advertising). In order to allay some of these concerns the Presidency suggests adding the word 'adversely'.

299 Presidency suggestion in order to ally concerns voiced by DE, ES and PL that this criterion was too broad. DE wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there also cases of automated data processing which actually were aimed at increasing the level of data processing (e.g. in case of children that are automatically excluded from certain advertising). In order to allay some of these concerns the Presidency suggests adding the word 'adversely'.

300 UK scrutiny reservation on whether the proposed exemptions in paragraph 2 are sufficient, and whether there are any unintended consequences arising out of the details of Article 20, especially on sectors such as the Credit Referencing Industry that rely on profiling (e.g. credit checks for the purposes of responsible lending).

301 BE proposal.

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

(b) is (…)[303] authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests[304]; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 (…)[305].

2. (…)

3. Profiling shall not be carried out:

(a) for direct marketing purposes unless pseudonymous data are processed and the data subject has not objected to the processing pursuant Article 19(2)[306];

(b) on special categories of personal data referred to in Article 9(1), unless Article 9(2) applies and subject to suitable measures to safeguard the data subject's legitimate interests[307] [308].

4. **(…) T**he information to be provided by the controller under Articles 14 and 14a shall include information as to the existence of profiling **referred to in paragraphs 1 and 3** and **information concerning** the logic involved **in the profiling, as well as the significance and** the envisaged consequences of such **profiling** of the data subject.

5. **(…)**

---

303 The word 'expressly' has been deleted further to the suggestion by BE, CZ and DE.

304 See revised recital 58.

305 Further to a suggestion by DE and IE, the reference to ' suitable safeguards' has been deleted as this resulted in a lack of clarity and added nothing to data protection requirements under Article 7.

306 COM reservation.

307 Regarding the original Commission proposal for paragraph 3 DK and UK queried why there couldn't be automated processing of health data (e.g. by insurance companies). FR and AT reservation on the compatibility with the E-Privacy Directive.

308 The Presidency would welcome an exchange of views on the usefulness of this paragraph. FR, AT, DK and SI had previously entered a scrutiny reservation on the word 'solely'; FR and DE had pointed out that 'not … solely' could empty this prohibition of its meaning by allowing sensitive data to be profiled together with other non-sensitive personal data.

SECTION 5
RESTRICTIONS

Article 21

Restrictions[309]

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5[310] and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society[311] to safeguard[312]:

   (aa) national security[313];

   (ab) defence[314];

   (a) public security;

   (b) the prevention, investigation, detection and prosecution of criminal offences[315];

---

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

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

311 CZ is opposed to these 'quasi-constitutional' qualifications to the requirement 'necessary'. LU proposed adding the qualification 'non-discriminatory', but the Presidency deems this is covered already by the proposed wording derived from the ECHR case law.

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

313 Addition at the suggestion CZ, DE, FI, NL, SE, SI and SK copied from the 1995 Data Protection Directive. FR and UK also sought clarification in this regard.

314 Addition at the suggestion CZ, DE, FI, SE, SI and SK copied from the 1995 Data Protection Directive. FR and UK also sought clarification in this regard.

315 SK thought this was in contradiction with the scope of the proposal (cf. Recital 16, Article 2(e)).

(c) other important objectives of general public interests of the Union or of a Member State[316], in particular[317] an important[318] economic or financial interest of the Union or of a Member State, including[319], monetary, budgetary and taxation matters and the protection of market stability and integrity;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions[320];

(e) a monitoring, inspection or regulatory function connected, even occasionally[321], with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(f) the protection of the data subject or the rights and freedoms of others[322].

2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to **the processing or categories of processing, its** purposes[323], **the scope of the restrictions introduced**[324], the specification of the controller and the safeguards, taking into account of **the nature, scope or purposes of the processing and the risks for the rights and freedoms of data subjects**[325].

316 DE, IT, LT scrutiny reservation as to the broad character of this exemption. SE thought it should be moved to a separate subparagraph.
317 UK, supported by NO, suggested to use the words 'including, but not limited to'
318 DK and UK scrutiny reservation on the adjective 'important'.
319 FR suggested adding ' public health'. The Commission's argued that this was already covered by subparagraph (f).
320 LU remarked that there were over 800 regulated professions in the EU.
321 LU remarked that the terms 'even occasionally' gave a very broad meaning to this derogation.
322 DE queried what is exactly covered by this subparagraph.
323 Further to IT proposal.
324 FR proposal.
325 DE scrutiny reservation regarding the exact impact of this paragraph.

CHAPTER IV

CONTROLLER AND PROCESSOR[326]

SECTION 1

GENERAL OBLIGATIONS

Article 22

***Responsibility of the controller*[327]**

1. Taking into account the nature, scope and purposes of the processing and the risks for the (..) rights and freedoms of data subjects[328], the controller shall (…) implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[329].

2. (…)[330]

---

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

327 UK thinks this Article should be deleted as it overlaps with existing obligations and focuses too much on procedures rather than on outcomes. DE, LT and PT deplored that Article 22 does not contain an exception for SMEs. BE remarked that anyone who puts a photo on social media might be considered as a controller. SK proposed introducing a new concept of 'entitled person' in Article 4 of the Proposal for a Regulation, together with obligations for the controller and processor to instruct their 'entitled persons' who come into contact with personal data about rights and obligations under this regulation as well as laying down responsibility for their infringement. An 'entitled person' could be defined as 'any natural person who comes into contact with personal data as part of his employment, membership, under the authority of elected or appointed, or in the exercise of public functions, which may process personal data only on the instruction of the data controller or representative of the data controller or the data processor'. COM stressed the need to have a general obligation on the controller's responsibility, which could be further elaborated in view of a risk-oriented element.

328 Whilst welcoming the introduction of a risk-based approach, several delegations stressed that the risk concept should be further detailed, either in the text of the Regulation itself (COM, DE, FR, HU, LU, NL, PT), possibly its recitals (IT, SE) or through guidance (maybe by the EDPB: ES) or codes of conduct (UK). DE pointed out that the text of the Regulation should allow differentiating the obligations on controllers by reference to the low or high degree of risk.

329 BE and IE have stated that there are dangers in maintaining such a vaguely worded obligation, applicable to all controllers, non-compliance of which is liable to sanctions.

330 The Presidency has deleted this paragraph as it deems that there is no need to repeat obligations which are spelt out later on in the Chapter

2a. Where proportionate in relation to the processing activities[331], the measures referred to in paragraph 1 shall include the implementation of:

(a) appropriate data protection policies by the controller[332];

(b) mechanisms to ensure that the time limits established for the erasure **and restriction** of personal data are observed[333].

3. (…) [334]

4. (…)[335].

[331] HU and PL thought this wording allowed too much leeway to delegations. AT thought that in particular for the respects to time limits (b) the reference to the proportionality was problematic.

[332] UK thought this was too complicated.

[333] Moved from Article 17.

[334] BE and CZ had pleaded for the deletion of the entire paragraph.

[335] COM reservation on deletion

Article 23

Data protection by design and by default[336]

1. Having regard to the state of the art and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope or purpose of the processing[337], the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself[338], implement (…) technical and organisational measures (…) appropriate to the activity being carried on and its objectives[339], including the use of pseudonymous data, in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of (…) data subjects.[340]

2. The controller shall[341] implement appropriate[342] measures for ensuring that, by default, only (…) personal data (…) which are necessary[343] for each specific purpose of the processing are processed; (…) this applies to the amount of (…) data collected, (...) the period of their storage and their accessibility[344]. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals[345] without human intervention.

---

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

337 Further to SE suggestion.

338 SK proposed referring to 'no later than prior to processing'.

339 ES proposal.

340 Some delegations (BE, NL) stated this paragraph added little in terms of legal obligations compared to other articles in the draft regulation. It might be moved to a recital.

341 FR suggested using exhortatory language instead of legally binding terms.

342 SE suggestion.

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

344 NL proposal aimed at to ensuring a better connection between the second and third sentence as well as an additional encouragement to data controllers to restrict access to data as much as possible.

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

2a. **The controller may demonstrate compliance with the requirements set out in paragraphs 1 and 2 by means of a certification mechanism pursuant to Article 39.**

3. (…)

4. (…)

Article 24

Joint controllers [346]

1. (…)[347] Joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a[348], by means of an arrangement between them[349] unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject[350].

---

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

347 CZ argued in favour of deleting 'conditions and means', except for subcontractors. UK suggested deleting 'conditions'.

348 NL proposal aimed at clarifying that joint controllers should also determine their respective duties under Article 14.

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

350 SE proposal. Cf. remarks made by FI and NL.

2. The data subject may exercise his or her rights under this Regulation in respect of and against each of the joint controllers[351].

Article 25

Representatives of controllers not established in the Union[352]

1. In the situation referred to in Article 3(2), the controller shall designate **in writing** a representative in the Union[353].

2. This obligation shall not apply to:

   (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41[354]; or

   (b) an enterprise employing fewer than 250 persons unless the processing it carries out involves high risks for the rights and freedoms of **data subjects, having regard to the nature, scope and purposes of the processing**[355]; or

---

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

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

353 SI reservation.

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

(c) a public authority or body[356]; or

(d) (…)[357].

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[358].

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.

---

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

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

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

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

Article 26

Processor[359]

1. (…)[360] The controller shall use only a processor providing sufficient guarantees[361] to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…)[362].[363]

2. [Where the processor is not part of the same group of undertakings as the controller[364],] the carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of data and categories of data subjects[365] or other legal act[366] binding the processor to the controller and stipulating in particular that the processor shall:

   (a) process the personal data only on instructions from the controller (…)[367], unless required to do so by Union or Member State law law to which the processor is subject[368];

   (b) (…)[369];

---

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

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

361 FR thought the 'sufficient guarantees' should be detailed.

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

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

364 Further to NL and SE remark that a processor who is part of the same group as the controller would not necessarily act on the basis of a contract. COM reservation; DE and IT scrutiny reservation: did not understand why they needed to be privileged.

365 Further to DE suggestion, 'in particular' was deleted as this may indeed convey the wrong expression that there may be cases where the processor can process data without instruction.

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

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

368 Addition to ensure consistency with Article 27 (as pointed out by BE, FR, ES, SI and UK).

369 This was deleted; all confidentiality requirements have now been inserted in Article 30.

(c) take all (…) measures required pursuant to Article 30[370];

(d) determine the conditions for enlisting another processor (…)[371];

(e) as far as (…) possible, taking into account the nature of the processing[372], assist the controller in[373] responding to requests for exercising the data subject's rights laid down in Chapter III;

(f) determine the extent to which[374] the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) (…) not process the personal data further after the completion[375] of the processing specified in the contract or other legal act, unless there is a requirement to store the data[376] under Union or Member State law to which the processor is subject;

(h) make available to the controller (…)[377] all information[378] necessary to demonstrate compliance with the obligations laid down in this Article.

3. The controller and the processor shall retain in writing or in an equivalent form[379] the controller's instructions and the processor's obligations referred to in paragraph 2[380].

4. (…)[381].

---

370 UK and IE thought there was an overlap with Article 30.

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

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

373 Further to DE proposal.

374 DE and UK remarked that the processor may not always be able to provide such assistance.

375 SI queried when processing was 'ended'. ES and NL thought there should be an obligation to return the data.

376 Further to NL and SE suggestion.

377 Deleted further to remarks by DE, FR and SI; the reference is already in Articles 29 and 53.

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

379 Further to the CZ, ES and NL demand that this should also encompass documentation in electronic form.

380 ES thought this requirement was excessively bureaucratic.

4a. The processor shall inform the controller if the processor considers that an instruction by the controller would breach the Regulation[382].

5. (…)[383]

Article 27

Processing under the authority of the controller and processor

(…) [384]

[381] UK thought this contradicts §2(a) and Article 27. Further to the remarks of BE, DK, DE, ES, FR, IT, NL, PT, SE and SI that this was an illogical consequence of violations of instructions, this paragraph was deleted. This does not detract from the possibility to impose sanctions on processors who have transgressed data protection rules by violating the instructions from the controller.

[382] Further to DE proposal. FR thought this might be problematic in a liability context.

[383] COM reservation on deletion.

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

Article 28

Records[385] ***of categories of processing activities*** [386]

1. Each controller (…)[387] and, if any, the controller's representative, shall maintain **a record regarding** all categories of processing activities[388] under its responsibility[389]. [390]This **record** shall contain (…)[391] the following information:

   (a) the name and contact details of the controller **and** any joint controller **(…),** controller's representative **and data protection officer**[392], if any;

   (b) (…)[393];

   (c) the purposes of the processing (…)[394];

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

   (e) the (…) **regular**[395] categories of recipients of the personal data (…);

---

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

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

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

388 Inspired by Article 18 of the 1995 Data Protection Directive: 'any wholly or partly automatic processing operation or set of operations intended to serve a single purpose'. BE and PL thought this could be further clarified in a recital.

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

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

391 Deletion at the proposal of CZ, FR, NL and SI.

392 Moved from subparagraph (b).

393 Moved to (a).

394 Deleted at the suggestion of the UK, as it overlaps with Article 6(1)(f). COM reservation on deletion.

395 FI proposal.

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation, (…)[396] [and, in case of transfers referred to in point (h) of Article 44(1), the **details** of appropriate safeguards]**[397]**;

(g) a general indication of the time limits for erasure of the different categories of data[398];

(h) (…)[399].

2a. Each processor[400] shall maintain a **record** of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor 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 and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards.

3. On request, the controller and the processor and, if any, the controller's representative, shall make the **record** available (…) to the supervisory authority[401].

---

396 HU reservation on deletion.

397 BE suggested referring to the legally binding instrument in case of a all transfers to a third country on the basis of articles 42 and 43.

398 ES and NL thought this should be done only where possible or relevant. FR and SI thought that the word 'general' should be deleted.

399 Deleted as it is already covered by Article 22(1).

400 UK thinks this article should not apply to processor(s at all, as all their processing activities are crried out under the responsibility of the controller.

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

4. The obligations referred to in paragraphs 1, (…) **to** 3 shall not apply to:

(a) (…)[402]

(b) an enterprise or a body employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities[403]; or

(c) categories of processing activities which[404] by virtue of the nature, scope or purposes of the processing[405] are unlikely to represent **high**[406] risks for , the rights and freedoms of data subjects

5. (…)

6. (…)

Article 29

Co-operation with the supervisory authority

(…)[407]

402 In view of the remarks by delegations (BE, DE, FR, NL, and LT) that this exception overlaps with the household exception of Article 2(d), this was deleted. Whilst COM has pointed out that the drafting of the latter is not identical with the drafting of Article 28(4) (a), it is difficult to see in which cases a natural person processing personal data without a commercial interest would not fall under the household exception and at any rate thinks that those cases should not be covered by the Regulation as such. COM reservation on deletion.

403 Many delegations criticised the appropriateness of this criterion: AT, BE, DE, ES, FR, GR, IT, LT, LU, NL, MT, PT, and SE. At the request of PL, AT and UK, COM clarified that concept of ancillary activities was aimed at inserting a risk-based approach into this criterion.

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

405 ES scrutiny reservation.

406 CZ proposal.

407 In view of the view held by several delegations (DE, ES, FR, NL, and SI, UK) that this article was superfluous in that controllers and processors obviously had a legal obligation to comply with requests made by data protection authorities under this Regulation, this Article was deleted. PT was in favour of retaining it.

SECTION 2
DATA SECURITY AND CONFIDENTIALITY

Article 30

Security and confidentiality[408] of processing[409] [410]

1. Having regard to the state of the art and the costs of their implementation and taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects[411], the controller and the processor[412] shall implement appropriate technical and organisational[413] measures including the use of pseudonymous data to ensure a level of confidentiality and security appropriate to these risks.

2. (…) [414].

2a. The controller may demonstrate compliance with the requirements set out in paragraph 1 by means of a certification mechanism pursuant to Article 39.

2b. Any person acting under the authority of the controller or the processor shall be bound by an obligation of confidentiality[415], which shall continue to have effect after the termination of their activity for the controller or processor[416].

3. (…).

---

408 IT reservation on the addition of confidentiality in this article. UK also thought it could be dealt with elsewhere

409 Several delegations (DE, FR, and IE) thought that more clarity was required as to what kind of risks for which actors were concerned. DE regretted the text of Article 17 of the 1995 Data Protection Directive had not been followed more closely. PT would have hoped for a more ambitious text. IT and UK pleaded in favour of an equivalent principle of data security in Article 5.

410 BE suggested adding a paragraph clarifying that the measures envisaged are covered by Article 6(1)(f). The Presidency thinks that this is superfluous in view of the legal obligation under the Regulation to take such measures.

411 FR suggested this be limited to the processing of sensitive data. FR also remarked that in this context the controller should rather evaluate security risks. Further clarification was required as what is to be understood by 'risk'

412 Several delegations thought that the controller should have the main responsibility (NO, NL, UK).

413 SK thought 'personal' measures should also be mentioned.

414 ES doubted the added value of this paragraph; NL, thought that this paragraph should be better aligned to paragraph 1. Therefore paragraphs 1 and 2 have been merged. NL wondered whether it would be possible to envisage different classes of data processing operations according the risk involved. UK suggested inserting a reference to

415 CZ queried where this obligation would be defined.

416 FR was examining any possible conflict with national labour laws and queried what was the link to Article 84.

4. (…). [417]

Article 31

Notification of a personal data breach to the supervisory authority [418]

1. In the case of a personal data breach which is likely to adversely affect the rights and freedoms of data subject**s** [419], the controller shall without undue delay and, where feasible, not later than 72 [420] hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51 [421]. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours [422].

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

2. **(…)** The processor shall alert and inform the controller **without undue delay** [423] **after becoming aware** of a personal data breach [424] [425].

---

417 Deleted in view of comments made by DE, ES, IT, LV, RO and UK. PL was in favour keeping the empowerments of paragraphs 4 and 5.

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

419 Inspired by E-Privacy Directive (Article 4(3)) in order to take account of the concern voiced by several delegations (BE, ES, IT, LU, PL, PT, RO, SE and SK) thought that the text should distinguish between minor and grave personal data breaches in order to avoid disproportionate administrative burdens both on data controllers and on data protection authorities BE scrutiny reservation. BG would have preferred a reference to a severe breach affecting a high number of individuals or a prevailing public interest The Presidency has endeavoured to clarify the meaning in the revised wording of recital 70.

420 Presidency proposal further to criticism by several delegations (BE, CZ, DE, ES, GR, MT, NL, LU, PT, SE, SI and UK). DE, ES, NL and UK would have preferred no specific time limit, but a reference to the absence of undue delay. COM, FR, IT and LU expressed concerns about the divergence with the E-Privacy regime, where the draft Commission Regulation on the measures applicable to the notification of personal data breaches (6503/13) provides for a 24-hour time period (and 4 days to inform the data subject).

421 Text further to UK remark that the territorial competence the DPA needed to be clarified and that a link with Article 51 needed to be made.

422 Many delegations thought that this Article places too much emphasis on notifying the data protection authority rather than on ensuring that the detrimental consequences of a personal data breach for the data subject: DE, DK, NL and SE. BE thought notification should not be required if the controller has applied appropriate measures to ensure the breach has no consequences.

423 Should 'the establishment' be replaced by 'after having become aware' as in paragraph 1?

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

425 De remarked that in view of the Commission proposal of 7 February 2013 for a Directive concerning measures to ensure a high level of network and information security across the Union (COM(2013) 48 final), it should be

3. The notification referred to in paragraph 1 must at least[426]:

(a) describe the nature of the personal data breach including**, where possible and appropriate**[427]**,** the categories and number of data subjects concerned and the categories and **approximate**[428] 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**[429] consequences of the personal data breach **identified by the controller**[430];

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

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach[431] .

3a. Where it is not possible to provide the information referred to in paragraph 3 (f) within the time period laid down in paragraph 1, the controller shall provide this information without undue further delay (…)[432].

---

checked whether in certain cases the authority competent for network and information security should also be notified.

426 ES proposed to replace the list by the following phrase: 'must have the necessary elements for the supervisory authority to assess the facts and their consequences and, where appropriate, remedial action to be taken'.

427 DE proposal.

428 BE proposal.

429 FI proposal. DE had proposed 'possible'.

430 FR proposal.

431 Copied from (c). Further to remarks by FR, GR and LU.

432 SI thought the 72-hour time period should apply only to the basic information and all other information could be provided at a later stage.

4. The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken[433].This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose[434].

[5. 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 establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[435]]

---

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

434 ES proposal to replace the last two sentences by: 'The controller shall operate a register of errors and incidents not referred to in paragraph 1 but with a relation to personal data processing, available for the supervisory authorities which may ask for a copy of it to be sent to them periodically'.

435 BE, DE, LT and UK pleaded for the deletion of paragraphs 5 and 6. ES, PT and NL asked for the deletion of paragraph 5.

Article 32

Communication of a personal data breach to the data subject[436]

1. When the personal data breach is likely to adversely affect the rights and freedoms of the data subject[437], the controller shall (…)[438] communicate[439] 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[440] 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)[441].

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

   a. the controller (…)[442] has implemented appropriate technological protection measures[443] and (…) those measures were applied to the data affected by the personal data breach, **in particular** those that[444] render the data unintelligible to any person who is not authorised to access it, such as encryption or the use of pseudonymous data[445] [446]; or

---

436 AT scrutiny reservation.NL thought there should be an exception for statistical data processing. FR thought that the possible application to public/private archives required further scrutiny.

437 BE and SK scrutiny reservation. SK wondered whether the controller is himself in a position to appreciate this.

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

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

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

441 ES thought it was sufficient to describe the nature of the personal data breach.

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

443 PL thought this required further clarification.

444 BE proposed 'have the purpose'.

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

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

b. **the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer at risk[447]; 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[448]; or

d. it would adversely affect a substantial public interest[449].

[4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so[450].]

[5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[451]]

---

447 Further to DE proposal.
448 Further to DE proposal.
449 Further ton FR proposal.
450 DE proposes to delete this paragraph.
451 BE, DE and UK pleaded for the deletion of paragraphs 5 and 6. BG, PT and ES asked deleting paragraph 5.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment [452]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific[453] risks for the rights and freedoms of data subjects[454], the controller or processor[455] shall, prior to the processing[456], carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. **(…)**[457].

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

---

452 FR thought that the possible application to public/private archives required further scrutiny.

453 ES thought that such assessment should not be required in all cases and wanted to restrict the scope of the Article. LU thought it would be useful to define such risks for the data subject (e.g. identify theft, financial loss etc). ES, FR, PT, RO, SK, SI and UK warned against the considerable administrative burdens flowing from the proposed obligation.

454 BE scrutiny reservation. De would have preferred to refer to the right to data protection.

455 BE, FR and PL reservation on reference to processor.

456 Addition so as to align the drafting to that of recital 70: GR.

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

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on automated processing and on which decisions[458] are based that produce legal effects concerning (…) data subjects or **adversly** affect data subjects[459];

(b) information on sex life, health, race and ethnic origin **(…),** where the data are processed for taking **(…)** decisions regarding specific individuals on a large scale[460];

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (…)[461] on a large scale[462];

(d) personal data in large scale **processing** systems **containing** genetic data or biometric data[463];

(e) other operations where (…) the competent supervisory authority considers that the processing is likely to present specific risks for the fundamental rights and freedoms of data subjects[464].

---

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

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

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

461 Reference to video-surveillance dropped in order to make the text more technology-neutral.

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

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

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

2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board. [465]

2b. Prior to the adoption of the list the supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union. [466]

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks for rights and freedoms of data subjects, the measures envisaged to address the risks[467], safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[468], taking into account the rights and legitimate interests of data subjects and other persons concerned[469].

4. (…)[470]

---

465 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2. BE and DE scrutiny reservation.

466 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2. BE and DE scrutiny reservation.

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

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

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

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

5. Where a controllers is a public authority or body[471] and where the processing pursuant to point (c) **or (e)**[472] of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[473].

[6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) [474].]

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

472 DE and FR proposal.

473 COM thinks the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

474 BE, FR, PT and ES asked for the deletion of paragraph 6; DE pleaded for the deletion of paragraphs 6 and 7.

Article 34

Prior (…) consultation[475] [476]

1. (…)[477]

2. The controller or processor[478] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a high degree of specific risks[479].

(…)

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation[480] (…) make appropriate recommendations to the data controller or processor[481]. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay[482].

---

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

476 BE suggested Article 34a: "*Member States may submit the processing of personal data concerning health, employment, social security and other by a public authority or body to a prior authorization by a DPA to prevent misuse of crossing data and to protect data subject rights*".

477 At the suggestion of several delegations (IT, SI, UK) this paragraph was moved to Article 42(6).

478 BE, LU and SI were opposed to mentioning the processor here. ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

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

480 BE suggestion. IT reservation on 6-weeks period.

481 SI reservation on the veto power of the DPA. Several delegations (DE, DK, NL, SE, SI) remarked that this sanctioning power was difficult to reconcile with the duty on controllers to make prior consultation under the previous paragraph. It was pointed out that this might lead to controllers avoiding to undertake data protection impact assessments. Several delegations (NL, PL, SI) queried how this veto power could be reconciled with the freedom of expression.

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

3a. During the period referred to in paragraph 3, the controller [or processor] shall not commence processing activities[483].

4. (…)

5. (…)[484]

6. **When consulting the supervisory authority pursuant to paragraph 2,** the controller or processor[485] shall provide the supervisory authority, on request, with the data protection impact assessment provided for in Article 33 and any (…) information **requested by** the supervisory authority **(…)**.[486].

7. Member States shall consult the supervisory authority during the preparation[487] of (…) legislative or regulatory measures which provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing (…).

[8. 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 determining the high degree of specific risk referred to in point (a) of paragraph 2.[488]]

9. (…)

---

483 BE, NL and PL reservation: this would amount to making the consultation into an authorisation and result in uncertainty for companies

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

485 BE was opposed to mentioning the processor here.

486 DE thought this paragraph should be deleted.

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

488 BG, FR, UK and DE pleaded for the deletion of paragraph 8. PL wanted to keep it.

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,**[489] designate a data protection officer (…)**.**

2. (…) **A** group of undertakings may appoint a single data protection officer[490].

3. Where the controller or the processor is a public authority or body[491], a single data protection officer may be designated for several (…) such authorities or bodies, taking account of their organisational structure and size[492].

4. (…) [493].

5. The (…) data protection officer **shall be designated** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37**.** (…) [494].

6. (…)[495].

---

489 Several Member States (BE, CY, DK, EE, ES, FR, IT, LT, PL, SE, SI, FI and UK) thought the appointment should not be mandatory and certainly not in all cases; reference was made in particular to the impossibility to appoint a DPO in all public authorities. It was also stated that the cost of appointing a DPO could be too high, especially for smaller entities in the public, but also in the private sector. NO believes that the appointment of a data protection officer can be useful in many cases, and supports the inclusion of an article on this in the regulation. NO thinks that the system should be mandatory only for public authorities who process sensitive data extensively. A substantial number of Member States (BE, CZ, FR, IT, NL, LV, LT, UK) thought that the function of DPOs should be a self-regulatory one without legally defined tasks and competencies. DE, BG and GR were in favour of the mandatory appointment of a DPO. AT scrutiny reservation. COM reservation on optional nature and deletion of points a) to c).

490 DE thought that there might be cases where one data protection officer might not be enough for large groups of undertakings. DE had suggested clarifying that 'if those undertakings act as a single unit for the purposes of contact with the outside world, if they regularly rely on processing within the group of undertakings and if the data subjects are not disadvantaged by the existence of a single data protection officer'. SI queried whether this would not endanger the independence of the DPO.

491 SK scrutiny reservation on this terminology.

492 FR demanded clarifications regarding 'organisational structure and size'.

493 Deleted in view of the optional nature of the appointment of the DPO.

494 Deleted in view of the optional nature of the appointment of the DPO.

495 Moved to Article 36, new paragraph 4, for systematic reasons.

7. (…) [496]. 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[497], be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her duties[498] **under paragraph 5**[499].

8. The data protection officer may be a staff member of the controller or processor, or fulfil his or her tasks on the basis of a service contract[500].

9. The controller or the processor shall **publish the** (…) contact details of the data protection officer **and communicate these** to the supervisory authority (…)[501].

10. Data subjects may **at any time**[502] 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[503].

11. (…).

Article 36

Position of the data protection officer[504]

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.

---

496 Deleted in view of the optional nature of the appointment of the DPO.

497 Presidency suggestion in order to allay concerns (DE, DK, GR, ES, FR, HU, IT, LV, SE, UK) regarding the interference with national labour law. FR scrutiny reservation.

498 BE proposed to replace the latter part of the sentence by a reference to positions expressed and the tasks accomplished by the DPO in his/her function.

499 UK thinks this paragraph should be deleted.

500 UK thinks this paragraph should be deleted.

501 FI thought 'to the public' should be reinstated. IT was opposed to making these details public. DE thought this paragraph could be deleted.

502 DE proposal.

503 DE proposed adding 'The data protection officer shall be required to keep confidential the identity of the data subject and any circumstances allowing their identity to be inferred, unless indicated otherwise by the data subject'.

504 COM clarified that its proposal for Article 36 and 37 were inspired by Regulation 45/2011. UK thought articles 36 and 37 could be deleted in a pure risk-based approach.

2. The controller or the processor shall support the data protection officer in performing the tasks **referred to in Article 37 by** provid**ing (…)**[505] resources necessary to carry out the duties **as well as access to personal data and processing operations**. (…)[506].

3. The controller or processor shall ensure that the data protection officer acts in an independant manner[507] with respect to the performance of his or her duties and tasks[508] and does not receive any instructions regarding the exercise of these **duties and tasks**. The data protection officer shall directly report to the highest management level of the controller or the processor[509]**.**

4. The data protection officer may fulfill other tasks and duties. The controller **or processor** shall ensure that any such tasks and duties do not result in a conflict of interests[510].

---

505 Deleted further to LT and FI remark.

506 AT, DE and NL had questioned the reference to the size of the controller, whereas the SME criterion was rejected.

507 ES and IT also thought the concept of independence was problematic in the context of the DPO.

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

509 BE suggested adding 'The data protection officer must ensure confidentiality of information obtained while performing his or her tasks, in particular as regards to information relating to complaints and information relating to the data processing activities of the controller or processor'. The Presidency believes this is already covered by the addition in paragraph 10 of Article 35.

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

Article 37

Tasks of the data protection officer[511]

1. The controller or the processor shall entrust the data protection officer **(…)** with the following tasks:

   (a) to inform and advise the controller or the processor **and the employees who are processing personal data**[512] of their obligations pursuant to this Regulation **(…);**

   (b) to monitor **compliance with**[513] this Regulation and **with** the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising[514] and training of staff involved in the processing operations, and the related audits[515];

   (c) (…);

   (d) (…);

   (e) (…);

   (f) (…)[516];

   (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[517];

---

511 UK thought this article could be deleted.
512 BE proposal.
513 BE proposal.
514 Further to PL and NL suggestion.
515 DE proposal.
516 DK, GR SE, SI and UK thought this list was much too detailed. In response to this, the Presidency suggests deleting subparagraphs (c) to (f) as these are all covered by (a) (and (b).
517 DE suggested deleting the reference to the initiative of the DPO.

(h) to act as the contact point for the supervisory authority on issues related to the processing, including the prior consulation referred to in Article 34, and consult with the supervisory authority, on his/her own initiative[518];

2. (….)[519].

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct [520]

1. The Member States, the supervisory authorities, **the European Data Protection Board** and the Commission shall encourage the [521]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 draw up codes of conduct, or amend or extent such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(a) fair and transparent data processing;

(b) the collection of data;

---

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

519 NL proposed adding two paragraphs: 3. The controller will entrust the data protection officer with to power to inspect any data processing operation carried out under his responsibility and the right of access to all data processed. 4. The data protection officer may not further process any data to which he has gained access in the exercise of his duty, except on instructions of the controller, unless he is required to do so by Union or Member State law .'

520 DE, FR and SI stated that this article should not apply to the public sector. DE made an alternative proposal, for this article 6413/13 DATAPROTECT 15 JAI 100 MI 107 DRS 24 DAPIX 18 FREMP 11 COMIX 98 CODEC 332.

521 ES proposed adding 'participatory'.

(ba) the use of pseudonymous data;

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

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

(e) information and protection of children;

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

(f) transfer of data to third countries or international organisations[522].

(g) (…)

(h) (…)

1b. Such a code of conduct shall contain mechanisms for monitoring and ensuring compliance with it by the controllers or processors which undertake to apply it, without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.

1c. In drawing up a code of conduct, associations and other bodies referred to in paragraph 1a shall consult, as appropriate, relevant stakeholders and in particular data subjects, and consider any submission received in response to their consultations.

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

2. Associations and other bodies **referred to in paragraph 1a** [523] which intend to draw up a code of conduct or to amend or extend an existing code of conduct may submit them to the supervisory authority **which is competent pursuant to Article 51. Where the code of conduct relates to processing activities in several Member States,** the supervisory authority **shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which** may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation.(…)[524].

2a. The European Data Protection Board shall register the codes of conduct and publish details of them.

3. **Where a code of conduct is drawn up by** associations and other bodies representing categories of controllers in several Member States, **the European Data Protection Board shall** submit **its opinion on the** code of conduct and on amendments or extensions to an existing code of conduct to the Commission(…)[525].

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union[526]. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4[527].

---

523 FR asks what is meant by this.

524 Based on national experiences, DE was sceptical as to the chance of success of this mechanism. IT and SE queried how to make the outcome binding.

525 BE, RO and SI proposal. DE, IE, ES, PT also remarked that the DPAs should be involved. ES thought that the Commission need not necessarily be involved.

526 FR scrutiny reservation regarding the legal status of such approved codes of conduct and in particular their binding nature.

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

Article 39

Certification[528]

1. (…) **The** Member States**, the European Data Protection Board**[529] **and** the Commissionshall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks **for procedures and products**[530], allowing data subjects to quickly assess the level of data protection provided by controllers and processors. (…)

2. A certificate may enable the controller to demonstrate compliance with the controller obligations under this Regulation, in particular the requirements set out in Articles 23 and 30 and the provision of mechanisms to facilitate data subject requests under Articles 15 to 19.

3. A certificate does not reduce the responsibility of the controller for compliance with this Regulation.

4. The controller which submits its processing to the certification mechanism shall provide the body referred to in Article 39a (1) with all information and access to its processing activities which are necessary to conduct the certification procedure. Where the processing concerns processing operations referred to in Article 33(2), the controller shall provide the data protection impact assessment to the body. The supervisory authority may request the controller in accordance with Article 33(2)(e) to carry out an impact assessment in order to support the assessment by the body.

---

528 CZ thought this Article should be deleted. DE, ES, FR, IT, NO and PT took a more favourable view, but thought the drafting was amenable to improvement. FR thought the terminology used was unclear an that the DPA should be in a position to check compliance with certified data protection policies; the Presidency will try to do this in Article 53.

529 DE proposal. ES, IT and UK thought the EDPB should be given a role here.

530 DE proposal.

5. The certification issued to a controller shall be subject to a periodic review by the body referred to in Article 39A(1). It shall be withdrawn where the requirements for the certification are not or no longer met.

Article 39a

Certification body and procedure

1. The certification and its periodic review shall be carried out by an independent certification body which has an appropriate level of expertise in relation to data protection and is accredited by the supervisory authority which is competent according to Article 51.

2. The supervisory authorities shall submit the draft criteria for the accredition of the body referred to in paragraph 1 to the European Data Protection Board under the procedure referred to in Article 57.

3. The body referred to in paragraph 1 shall act in an independent manner with respect to certification, without prejudice to the duties and powers of the supervisory authority. The body shall ensure that its tasks and duties do not result in a conflict of interest. The data protection certification mechanism shall set out the procedure for the issue, periodic review and withdrawal of data protection seals and marks.

4. The body referred to in paragraph 1 shall be liable for the proper assessment leading to the certification, without prejudice to the responsibility of the controller for compliance with this Regulation.

5. The body referred to in paragraph 1 shall inform the supervisory authority on certifications issued and withdrawn and on the reasons for withdrawing the certification.

6. The criteria for the certification and the certification details shall be made public by the supervisory authority in an easily accessible form.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and **revocation**, and requirements for recognition **of the certification and the requirements for a standardised 'European Data Protection Seal'** within the Union and in third countries.

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)[531].

_____

[531] DE pleaded in favour of deleting the last two paragraphs.