COUNCIL OF THE EUROPEAN UNION

Brussels, 6 May 2013

Interinstitutional File: 2012/0011 (COD)

8004/2/13 REV 2

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 revised draft of the text of Chapters I to IV was discussed at DAPIX meetings of 9-11, 24 and 29-30 April 2013. On the basis of these discussions, the Presidency has endeavoured to further redraft the text of these Chapters. Obviously any changes made are *ad referendum,* subject to further scrutiny by all delegations (including the Commission).

4. All changes made to the original Commission proposal are underlined text, or, where text has been deleted, indicated by (…). New changes (as compared to 8004/13) are indicated **in underlined bold text**. Where existing text has been moved, this text is indicated *in italics*.

5. As articles 2, 3 5, 7 and 9(1)(a) (and relevant recitals) have been submitted to COREPER for political guidance, these articles are not contained in the annex to this note.

6. The following delegations have a general scrutiny reservation on the revised draft of Chapters I-IV: FR, LV, AT, PT, RO, SE, FI and SK. 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 conduct the third examination of Chapters I - IV with a view to reaching a general approach on these Chapters at the June Council meeting.

---

1 BE, CZ, DK, EE, HU, 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.

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[2],

After consulting the European Data Protection Supervisor[3],

Acting in accordance with the ordinary legislative procedure,

---

2 OJ C, p. . .

3 OJ C p. .

Whereas:

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

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

3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

3a) (…) The right to the protection of personal data is not an absolute right**; it** must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.

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

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

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

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

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

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

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

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

11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. **The proper functioning of the internal market requires that the free movement of personal data between Member States should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.** To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

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

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

……..

23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, **taking into consideration both available technology** at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information**, that is information** which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes. The principles of data protection should not apply to deceased persons.

24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not **(…)** be considered as personal data (…) **, if they do not identify an individual or make an individual identifiable.** [5].

……

25a) **Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained[6].**

---

5 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.

6 New recital in order to clarify the definition of Article 4 (10)

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

27) [The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.]

28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. (…)[7].

……..

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

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

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

---

7 COM reservation against deletion of the reference to the UN Convention on the Rights of the Child.

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

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

40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific (…) purposes. **In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the consequences of the intended further processing for data subjects (…), and appropriate safeguards (…).** Where the **intended** other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured. **Further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.**[8]

41) Personal data which are, by their nature, particularly sensitive **(…)** in relation to fundamental rights **and freedoms**, deserve specific protection. This should also include **personal data** revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless the data subject gives his **or her** explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

[8] Further to NL proposal.

42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where **important** grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historcal, statistical and scientific (…) purposes. **A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.**

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

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

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

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

47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, **(…)** in particular access to data, rectification, erasure and to exercise the right to object. Thus the controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons **where the controller** does not **intend to** comply with the data subject's request.

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

49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. **Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner[9].**

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

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

[9] Further to BE proposal.

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. (…)[10] A controller should not retain personal data for the sole purpose of being able to react to potential requests.

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

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

[10] Deleted as it overlaps with recital 45.

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

55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application (…)[11] into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. **The right to transmit the data into another automated processing system should not imply the erasure of personal data which have been provided by the data subject for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. By its very nature this right cannot be exercised against controllers processing data in the exercise of their public duties.**

56) In cases where personal data might lawfully be processed **(…)**on grounds of 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. **It** should be **for** the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

[11] IT doubted whether this right could be exercised against social networks, in view of the household exemption.

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

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

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

60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures to **(…)** be able to demonstrate the compliance of **categories of** processing **activities** with this Regulation, **such as keeping a record, implementing technical and organisational measures for ensuring an appropriate level of security or performing a data protection impact assessment. These measures should take** into account the nature, scope**, context** and purposes of the processing and the risks for the rights and freedoms of data subjects. **Such risks are presented by data processing which could lead to physical, material or moral damage, in particular:-**

- **where individuals might be deprived of their rights or from control over their personal data;**
- **where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;**
- **where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;**
- **where personal data of vulnerable individuals, in particular of children, are processed;**
- **where processing involves a large amount of personal data and affects a large number of data subjects; or**
- **where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage[12].**

[12] Further to FR proposal.

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

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

60c. Guidance for the implementation of such measures by the controller **[or processor], especially as regards the identification of the risks, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks**[13]**,** could be **provided** in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board **or through the designation of a data protection officer or,** where a data protection impact assessment indicates that processing operations involve a high degree of specific risks, through consultation of the supervisory authority prior to the processing.

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

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

---

13 FR proposal.

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour **in the Union**, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise **unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing** or is **a** public authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.

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

64) (…).

(64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to present specific risks **for the rights and freedoms of data subjects**, the controller [or the processor] **should** be responsible **for the carrying out of** a data protection impact assessment to evaluate, **in particular, the origin, nature, likelihood and severity of these risks**. The outcome of the assessment **should** be taken into account when determining the (…) appropriate measures to **be taken in order** to demonstrate that the processing of personal data is in compliance with this Regulation.

65) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the **specific** risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, **including confidentiality,** taking into account **available technology** and the costs of **(…)** implementation in relation to the risks and the nature of the personal data to be protected. **(…)**.

67) A personal data breach may, if not addressed in an adequate and timely manner, result in **severe material or moral harm to individuals such as loss of control over their personal data or the limitation of their rights, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy**[14] or any other economic or social disadvantage (…) to the individual concerned. Therefore, as soon as the controller becomes aware that **(…)**. a **personal data** breach has occurred **which may result in severe material or moral harm** the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot **be** achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be **severely** affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as **severely** affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, (…) to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

---

14 Further to FR proposal.

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

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

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

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation**s** should be abolished, and replaced by effective procedures and mechanism**s** which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes **(…).** In such cases, a data protection impact assessment should be carried out by the controller [or processor] prior to the processing **in order to asses the severity and likelihood of these specific risks, taking into accpunt the nature, scope and purposes of the processing and the sources of the risks**, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

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

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

73) Data protection impact assessments **may** be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.

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

75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person with expert knowledge **of data protection law and practices** may assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

76) Associations or other bodies representing categories of controllers **or processors** should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could callibrate the obligations of controllers and processors, taking into account the risks inherent to the processing for the rights and freedoms of data subjects.

76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data[15].

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

3. The free movement of personal data **between** **Member States** shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.[16] [17].

……..

15 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.

16 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. DE and NL remarked that the drafting did not specify the addressees of this rule. DE also wondered why this rule could not cover intra-Member State transfers. 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.

17 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. 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.

Article 4

Definitions

For the purposes of this Regulation:

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

(2) (…);

(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[18];

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

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, or erasure[19];

(3a) 'restriction of processing' means **the marking of stored** personal data **with the aim of limiting their processing in the future**[20];

(4) (…)[21];

(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[22] 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;

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

---

19 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.

20 At the suggestion of DE (supported by SE and SK), the presidency has copied the definition from the proposed data protection directive. HU also thought the previous definition was too narrow and AT was concerned that the limitation to storage would create 'data graveyards'

21 This was deleted as it was a completely outdated concept and it was now deleted from Article 2(1)

22 UK suggests deleting the reference to the conditions and the means of processing, as this is normally for the processor to determine, not for the controller and reverting to the formulation under the 1995 Directive.

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

[(6a) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;]

(7) 'recipient' means a natural or legal person, public authority, agency or any other body **other than the data subject, the data controller or the data processor**[24] to which the personal data are disclosed**;**[25] **however regulatory authorities which may receive personal data in the exercise of their functions shall not be regarded as recipients.**

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[26];

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual **that have been inherited or acquired, resulting** from an analysis of a biological sample from the individual in question, (…)[27;]

---

24 HU, IT, LU and PL proposal.

25 DE and PT reservation. 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.

26 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'.

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

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which **confirms the**[28] (…) unique identification of that individual, such as facial images, or dactyloscopic data[29];

(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 individual[30];

(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[31];

---

28 CZ proposal.

29 SE and AT scrutiny reservation. SI did not understand why genetic data were not included in the definition of biometric data.. FR queried the meaning of 'behavioural characteristics of an individual which allow their unique identification'. 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.

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

31 CZ and SE scrutiny reservation. COM reservation.

(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[32];.

- 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;[33]]

(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 34;

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

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings[35];

---

32 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.

33 This definition will be revisited when discussing Chapter V.

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

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

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

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

(19) 'supervisory authority' means a[36] public authority which is established by a Member State pursuant to Article 46;

(…)[37];

(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[38] [39] [40].

……..

[36] FR proposal, supported by SI, to add 'independent'.

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

[38] OJ L 204, 21.7.1998, p. 37–48.

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

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

CHAPTER II

PRINCIPLES

Article 6

Lawfulness of processing[41]

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[42];

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

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

   (d) processing is necessary in order to protect the vital interests[43] of the data subject **or another person**[44];

   (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[45] [46];

---

41 IT, AT, PT and SK scrutiny reservation.

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

43 See also revised recital 37.

44 UK preferred the wording of the 1995 DPD.

45 COM clarified that this was the main basis for data processing in the public sector. DE, DK 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.

46 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[47] pursued by the controller or by a controller to which the data are disclosed [48] except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties[49] [50].

2. (…)

3. The basis for the processing referred to in points (c) and (e)[51] of paragraph 1 must be provided for in:

(a) Union law, or

(b) **national** law of the Member State[52] to which the controller is subject.

---

47 FR and LT scrutiny reservation.

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

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

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

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

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

The purpose of the processing shall be determined in this legal basis **or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the authority**. 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.[53]

3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account:

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

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

(c) the nature of the personal data;

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

(e) appropriate safeguards [54].

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) [55] of paragraph 1[56].[57].

5. (…)[58].

---

53 DK and DE scrutiny reservation.

54 Partially based on NL proposal.

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

56 DE, IT, NL and PT scrutiny reservation.

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

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

Article 8

Processing of personal data of a child[59]

1. (…) **Where Article 6 (1)(a) applies**, in relation to the offering of information society services directly to a child[60], the processing of personal data of a child below the age of 13 years[61] shall only be lawful if and to the extent that **such consent** is given or authorised by the child's parent or guardian**.**

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

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child[62].

---

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

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

61 Several delegations queried the expediency of setting the age of consent at 13 years: DE, FR, HU, LU, LV and SI. DE and RO proposed 14 years; SI 15 years. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA).

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

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(…)[63].

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)][64].

Article 9

***Processing of special categories of personal data*[65]**

1. The processing of personal data, revealing **racial** or ethnic origin, political opinions, religion or philosphical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences[66] or related security measures shall be prohibited.[67]

63 ES, FR and SE scrutiny reservation.

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

65 AT and NL 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 and pleaded in favour of a risk-based approach to sensitive data. SK and RO thought the inclusion of biometric data should be considered. COM opined that the latter were not sensitive data as such. SK also leaded in favour of the inclusion of national identifier. COM referred to the general discussion on an open versus closed list of sensitive data.

66 EE reservation: the inclusion of criminal convictions criminal offences is contrary to the publicity of the functioning of the courts in accordance with Article 6 ECHR.

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

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

……

(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[68]; or

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

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

(e) the processing relates to personal data which are manifestly made public[69] by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims[70]; or

---

68 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.

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

70 Deletion of 'or otherwise' at the request of ES, IT, LV, LT, AT, RO. The Presidency has endeavoured to clarify the scope of this point further in recital 42.

(g) processing is necessary for the performance of a task carried out for reasons of **important**[71] public interest, on the basis of Union law or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests[72];

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81[73]; or

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

(j) (…)

2a *Processing of data relating to criminal convictions and offences*[74] *or related security measures* ***may be*** *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* ***reasons of important*** *public interest* ***(…),*** *and in so far as authorised by Union law or Member State law providing for adequate safeguards* **for the rights and freedoms of data subjects[75]. A complete register of criminal convictions may be kept only under the control of official authority.**

---

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

72 Moved from paragraph 2 (g).

73 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.

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

75 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.

3. (…)

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (…) additional information in order to identify the data subject for the sole purpose of complying with (…) this Regulation.[76].

2. Where, in such cases the controller does not know the identity of the data subject, articles 15, 16, 17, 17a, 17b, 18 and 19 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information allowing his or her identification[77].

[76] AT, DE, ES, FR, HU and UK scrutiny reservation.
[77] Further to BE proposal. COM scrutiny reservation.

CHAPTER III
RIGHTS OF THE DATA SUBJECT[78]

SECTION 1

TRANSPARENCY AND MODALITIES

Article 11
Transparent information and communication

1. (…)

2. (…).

Article 12
Transparent information, communication and modalities for exercising the rights of the data subject[79]

1. The controller shall take appropriate measures to provide any information referred to in Articles 14, 14a and 20(4) and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language **(…)**[80]**.** The information shall be provided in writing, or where appropriate, electronically or by other means.

1a[81]. The controller shall facilitate the **exercise** of data subject **rights** under Articles 15 to 19 (…). **(…)**.

---

78 General scrutiny reservation by UK on the articles in this Chapter.
79 DE SE, SI and FI scrutiny reservation.
80 COM reservation on deletion.
81 SI and UK thought this paragraph should be deleted.

2. The controller shall provide the information referred to in Articles 15 and 20(4) and information on action taken on a request under Articles 16 to 19[82] to the data subject without undue delay and at the latest within one month of receipt of the request[83] (…). This period may be extended for a further two months when necessary, taking into account the complexity of the request and the number of requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.

3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action[84] and on the possibility of lodging a complaint to a supervisory authority (…).

4. Information provided under Articles 14 **and** 14a **(…)** and any communication under Articles **16** to **19** and 32 shall be provided free of charge[85]. Where requests from a data subject are (…)[86] *manifestly* unfounded or excessive, in particular because of their repetitive character, the controller (…) may **refuse to act on** the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request.

---

82 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.

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

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

85 In the context of Article 15, CZ, DE, DK, LV, LT, SK, SI and UK argued that controllers should be allowed to charge a nominal fee.

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

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.

5. (…).

6. (…).

Article 13

Rights in relation to recipients

(...)

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14

Information to be provided where the data are collected from the data subject[87]

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

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

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

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

1a. In addition to the information referred to in paragraph 1, the controller shall[88] provide the data subject with any further information necessary to ensure fair and transparent[89] processing in respect of the data subject[90], having regard to the specific circumstances **and context** in which the personal data are processed **(…)**[91]:

(a) (…)[92];

(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[93];

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

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data **or restriction of processing of personal data** concerning the data subject and to object to the processing of such personal data, [including for direct marketing purposes[94]];

---

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

89 DK argued for the deletion of 'transparent'

90 FR scrutiny reservation

91 HU thought the legal basis of the processing should be included in the list. COM reservation on deletion.

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

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

94 FR and SE questioned whether it was necessary to single out this sector.

(f) the right to lodge a complaint to a supervisory authority (…)[95];

(…)

(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[96]; and

(h) the existence of profiling referred to in Article 20(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.[97]

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. (…).

---

95 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. FI insisted on including them

96 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. IT agreed for moving this to paragraph 1.

97 Moved from Article 20(4).

Article 14 a

Information to be provided where the data have not been obtained from the data subject[98]

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

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

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

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with any further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances **and context** in which the personal data are processed, (…)[99]:

   (a) the categories of personal data concerned;

   (b) (…)

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

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

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

---

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

99 HU thought the legal basis of the processing should be included in the list. COM reservation on deletion.

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

(g) the origin of the personal data, unless the data originate from publicly accessible sources[100];

(h) the existence of profiling referred to in Article 20(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.[101]

3. The controller shall provide the information referred to in paragraphs 1 and 2[102]:

(a) (…) within a reasonable period[103] after obtaining the data, having regard to the specific circumstances in which the data are processed, or

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

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

(a) the data subject already has the information; or

---

100 COM and AT scrutiny reservation.

101 Moved from Article 20(4).

102 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.

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

(b) the provision of such information in particular when processing personal data for historical, statistical or scientific purposes[104] proves impossible or would involve a disproportionate effort **or is likely to render impossible or to seriously impair the achievement of such purposes;[105] i**n such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[106], for example by using pseudonymous data[107]; or

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

(d) where the data originate from publicly available sources[108]; or

(e) where the data must remain confidential in accordance with a legal provision or **because** of the overriding legitimate interests of **another person**[109].

5. (…).

6. (…).

---

104 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.

105 BE proposal. COM scrutiny reservation.

106 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.

107 BE and IT reservation on the mentioning of pseudonymous data. BE suggested inserting a reference to Article 83.

108 COM reservation.

109 COM and AT reservation on (d) and (e).

Article 15

Right of access for the data subject[110]

1. The data subject shall have the right to obtain from the controller at reasonable intervals, on request, **and without an excessive charge**[111]**,** 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 **provide a copy of** the personal data undergoing processing and the following information to the data subject:

   (a) the purposes of the processing[112];

   (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[113];

   (d) **where possible**, the envisaged[114] 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 (…)[115] [116];

---

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

111 COM reservation.

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

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

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

115 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.

116 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[117], any available information as to their source[118];

(h) in the case of decisions referred to in Article 20, knowledge of the logic involved[119] in any automated data processing as well as the significance and envisaged consequences of such processing[120].

1a. Where personal data are transferred to a third country, the data subject shall have the right to obtain a copy of the appropriate safeguards relating to the transfer[121];

2. (…)Where personal data supplied **by the data subject** are processed by **automated** means and in a structured and commonly used format, the controller shall **on request** provide a copy of the data **concerning the data subject** in that format to the data subject[122].

3. (…).

4. (…).

5. [The rights provided for in **this** Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met][123].

---

117 DE proposal.

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

119 PL pleaded for excluding the underlying algorithm.

120 NL scrutiny reservation. DE thought this should be made more concrete. CZ and FR likewise harboured doubts on its exact scope.

121 Partially based on BE proposal.

122 COM, ES and FR thought this was too narrowly drafted. DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.

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

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[124]

1. (…) The data subject shall have the right[125] to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…) statement.

2. [The rights provided for in **this** Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.][126]

---

124 DE and UK scrutiny reservation.

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

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

Article 17
Right to be forgotten and to erasure[127]

1. The (…) controller[128] shall have the obligation to erase personal data without **undue** delay (…) and the data subject shall have the right to obtain the erasure of personal data without **undue** delay (…) where one of the following grounds applies:

---

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

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

(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) (…) 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;

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[129].

2. (…).

[129] RO scrutiny reservation.

2a. *Where the controller[130] (...) has made the personal data public[131] and is obliged pursuant to paragraph 1 to erase the data,* **the controller, taking account of available technology,** *shall take* ***(…)*** *reasonable steps[132], including technical measures,* ***(…)*** *to inform controllers[133] which are processing* **the** *data, that a data subject requests them to erase any links to, or copy or replication of that personal data[134].*

3. Paragraph**s** 1 **and 2a** shall not apply[135] 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[136];

---

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

131 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.

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

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

134 BE, ES, P 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 (DE, LU, NL, PL, PT, SE SI) had doubts on the enforceability of this rule.

135 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.

(b) *for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject*[137] **or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller**[138];

(c) for reasons of public interest in the area of public health in accordance with Article 81[139];

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

(e) (…);

(f) (…);

(g) **for the establishment, exercise or defence of legal claims**[140].

4. **(…)**.

5. (…).

---

136 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.

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

138 COM scrutiny reservation.

139 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.

140 Further to NL suggestion.

Article 17*a*

Right to restriction of processing

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

   (a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[141];

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

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

2. (…)

3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's **consent** or for the establishment, exercise or defence of legal claims (…) or for the protection of the rights of another natural or legal person or for reasons of **important** public interest[142].

4. **A data subject who obtained the restriction of processing pursuant to paragraph 1(a) or (c) shall be informed by the controller before the restriction of processing is lifted**[143]. (…)

---

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

142 ES asked who was to define the concept of public interest.

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

5. (…).

5a. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.][144].

Article 17b

Notification obligation regarding rectification or erasure [145]

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

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

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

Article 18

Right to data portability[146]

1. (…).

2. Where the data subject has provided personal data and the processing**, (…)** based on consent or on a contract[147], **is carried on in an automated processing system,** the data subject shall have the right to **withdraw these data in a form which permits the data subject to transmit them[148] into another automated processing system without hinderance from the contrller from whom the personal data are withdrawn** .

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

[3. The Commission may specify (…) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).][149]

---

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

147 BE, DE, FR IE, NL, 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. The Presidency has endeavoured to clarify this in recital 55.

148 Reinstatement of this requirement from the original proposal, at the suggestion of CZ and ES.

149 FR reservation: this would better set out in the Regulation itself.

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 .][150].

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19
Right to object[151]

1. The data subject shall have the right to object, on reasoned[152] 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 points (e) and (f) of Article 6(1)[153]**; 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[154] [155].

---

150 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.

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

152 COM reservation.

153 UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. ES and LU queried why Article 6(1) (c) was not listed here.

154 SE scrutiny reservation: SE and NL queried the need to put the burden of proof on the controller regarding the existence of compelling legitimate grounds. DE and FI queried the need for new criteria, other than those from the 1995 Directive. 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. 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.

155 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 and HU likewise thought that the reference to Article 6(e) should be deleted.

1a. (…)[156] Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)[157] process the personal data concerned except for the establishment, exercise or defence of legal claims[158].

2. Where personal data are processed for direct marketing[159] purposes, the data subject shall have the right to object free of charge at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…) and shall be presented clearly and separately from any other information[160].

2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed **for such purposes**[161].

3. (...).

---

156 The cross-reference in paragraph 1 to Article 17a obviates the need for paragraph 1a.

157 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'.

158 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.

159 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.

160 At the request of several delegations (FR, LT, PT), COM confirmed that this paragraph was not meant to create an opt-in system and that the E-Privacy Directive would remain unaffected. 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.

161 DE reservation.

4. [The rights provided for in **this** Article do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met[162]].

Article 20

Decisions based on profiling[163]

1. Every data subject shall have the right not to be subject to a decision based **solely** on profiling[164] *which produces legal effects* concerning him or her (…) or adversely[165] affects (…) him or her unless such processing:

---

162 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.

163 ES, FR, SE and UK scrutiny reservation. COM reservation. 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).

164 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.

165 DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there 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).

(a) is carried out in the course of the entering into, or performance of, a contract between the data subject and a data controller (…) and suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the rights of the data subject to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision [166]; or

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

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

2. (…).

3. Profiling shall not (…):

(a) *be carried* **on** for direct marketing purposes unless **suitable measures to safeguard the data subject's legitimate interests, such as the processing of** pseudonymous data**,** (…) **are in place** and the data subject has not objected to the processing pursuant Article 19(2)[167];

166 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.

167 ES, FR and NL scrutiny reservation: these delegations thought point (a) was drafted too narrowly.

(b) **be based** on special categories of personal data referred to in Article 9(1), unless Article 9(2) applies and **(…)** suitable measures to safeguard the data subject's legitimate interests [168] **are in place**.

4. (…)[169].

5. (…).

[168] BE, COM, FR, NL, AT and UK reservation; DK and PL scrutiny reservation. FR and AT reservation on the compatibility with the E-Privacy Directive. BE would prefer to reinstate the term 'solely based' regarding point (b), but FR and DE had previously pointed out that 'not … solely' could empty this prohibition of its meaning by allowing sensitive data to be profiled together with other non-sensitive personal data.

[169] At the suggestion of DE, this has been moved to Articles 14 and 14a.

SECTION 5
RESTRICTIONS

Article 21

Restrictions[170]

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[171] and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard[172]:

   (aa) national security;

   (ab) defence;

   (a) public security;

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

---

170 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.

171 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.

172 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.

(c) other important objectives of general public interests of the Union or of a Member State[173], in particular an important[174] economic or financial interest of the Union or of a Member State, including[175], monetary, budgetary and taxation matters and the protection of market stability and integrity;

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

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

(f) the protection of the data subject or the rights and freedoms of others[176].

2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to *the purposes* of the processing or categories of processing, the scope of the restrictions introduced, the specification of the controller **or categories of controllers[177]** and the **applicable** safeguards taking into account of the nature, scope **and** purposes of the processing and the risks for the rights and freedoms of data subjects.

---

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

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

175 FR suggested adding ' public health'. The Commission's argued that this was already covered by subparagraph (f).

176 DE queried what is exactly covered by this subparagraph.

177 NL proposal.

CHAPTER IV

CONTROLLER AND PROCESSOR[178]

SECTION 1
GENERAL OBLIGATIONS

Article 22

***Obligations of the controller*[179]**

1. Taking into account the nature, scope and purposes of the processing and the risks for the (..) rights and freedoms of data subjects[180], the controller shall (…) implement

---

178 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)

179 FR and UK thought this Article could be deleted as it overlaps with existing obligations. UK thought it focuses too much on procedures rather than on outcomes. DE, LT and PT deplored that Article 22 does not contain an exception for SMEs. BE remarked that anyone who puts a photo on social media might be considered as a controller. SK proposed introducing a new concept of 'entitled person' in Article 4 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.

180 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.

appropriate measures **and**[181] be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[182].

2. (…)

2a. Where proportionate in relation to the processing activities[183], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller[184];

(…).

2b. Compliance with the obligations of the controller may be verified by means of a certification mechanism pursuant to Article 39 or, where proportionate, may be carried out by internal or external auditors.

3. (…).

4. (…).

---

181 Deleted at the suggestion of BE.

182 BE and UK 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.

183 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.

184 UK thought this was too complicated.

Article 23

Data protection by design and by default[185]

1. Having regard to the **available technology** and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope **and** purpose of the processing, the controller shall (…), implement (…) technical and organisational measures (…) appropriate to the activity being carried on and its objectives, including the use of pseudonymous data, in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of (…) data subjects.[186]

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are **not excessive**[187] for each specific purpose of the processing are processed; (…) this applies to the amount of (…) data collected, (...) the period of their storage and their accessibility. **Where the purpose of the processing is not intended to provide the public with information,** those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals[188].

---

185 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.

186 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.

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

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

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

3. (…)

4. (…)

Article 24

Joint controllers [189]

1. (…) Joint controllers shall **in a transparant manner** determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them[190] unless, **and in so far as,** the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

---

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

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

2. **Irrespective of the terms of the arrangement referred to in paragraph 1, t**he data subject may exercise his or her rights under this Regulation in respect of and against each of the **(…)** controllers[191] **unless the data subject has been informed in a transparant manner which of the joint controllers is responsible.**

Article 25

Representatives of controllers not established in the Union[192]

1. In the situation referred to in Article 3(2), the controller shall designate in writing a representative in the Union[193].

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[194]; or

---

191 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.

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

193 SI reservation.

194 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

(b) an enterprise employing fewer than 250 persons unless the processing it carries out involves **specific** risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing[195]; or

(c) a public authority or body[196]; or

(d) (…)[197].

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[198].

3a. The representative shall be mandated by[199] 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.

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.

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

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

197 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

198 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.

199 BE proposed to state 'is liable'.

Article 26

Processor[200]

1. (…)[201] The controller shall use only processor**s** providing sufficient guarantees[202] to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…)[203].[204]

1a. The provision of sufficient guarantees referred to in paragraph 1 may be demonstrated by means of a certification mechanism pursuant to in Article 39.

2. The carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of data and categories of data subjects[205] or other legal act[206] 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 (…)[207], unless required to do so by Union or Member State law to which the

---

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

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

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

203 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.

204 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

205 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.

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

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

processor is subject [**and in such a case, the processor shall notify the controller unless the law prohibits it**[208]];

(b) (…);

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

(d) determine the conditions for enlisting another processor (…)[209];

(e) as far as (…) possible, taking into account the nature of the processing[210], assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;

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

(g) (…) **return** the personal data after the completion[211] of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;

(h) make available to the controller (…) all information[212] necessary to demonstrate compliance with the obligations laid down in this Article.

3. **The contract referred to in paragraph 2 shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.**

4. (…).

---

208 BE proposal.

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

210 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.

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

212 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.

5. (…)[213].

[213] COM reservation on deletion.

Article 27

Processing under the authority of the controller and processor

(…) [214]

Article 28

Records[215] of categories of personal data processing activities [216]

1. Each controller (…)[217] and, if any, the controller's representative, shall maintain a record **of** all categories of **personal data[218]** processing activities under its responsibility[219]. [220]This record shall contain (…)the following information:

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

   (b) (…);

---

214 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.

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

216 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.

217 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.

218 BE and IT proposal.

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

220 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.

(c) the purposes of the processing, including the legitimate interest when the processing is based is based on Article 6(1)(f)[221];

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

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

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation, (…)[222] (…)

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

(h) (…)

2a. Each processor[223] shall maintain a **record** of all categories of **personal data** processing activities carried out on behalf of a controller, containing:

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

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

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

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

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

---

221 UK suggested deleting it, as it overlaps with Article 6(1)(f).

222 UK reservation.

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

3. On request, the controller and the processor and, if any, the controller's representative, shall make the record available (…) to the supervisory authority[224].

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

(a) (…)[225]

(b) an enterprise or a body employing fewer than 250 persons**, unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing**[226]; or

(c) categories of processing activities which[227] by virtue of the nature, scope or purposes of the processing are unlikely to represent **specific** risks for the rights and freedoms of data subjects.

5. (…)

6. (…).

Article 29

Co-operation with the supervisory authority

(…)[228]

---

224 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.

225 COM reservation on deletion.

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

227 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

228 PT and ES scrutiny reservation on deletion.

SECTION 2
DATA SECURITY

Article 30

Security of processing

1. Having regard to the **available technology** and the costs of implementation and taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor[229] shall implement appropriate technical and organisational measures including the use of pseudonymous data to ensure a level of security appropriate to these risks.

2. (…).

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

2b. The controller **and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law[230].**

3. (…).

4. (…).

Article 31

Notification of a personal data breach to the supervisory authority[231]

1. In the case of a personal data breach which is likely to **severely** affect the rights and freedoms of data subject**s**[232], the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal

---

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

230 Text copied from Article 16 of the 1995 Directive.

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

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

data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)**(a) and** (b)[233].

2. (…) The processor shall alert and inform the controller without undue delay after becoming aware of a personal data breach[234] [235].

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

(a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and approximate number of data records concerned;

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

(c) (…) ;

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

(e) 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 .

---

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

234 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.

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

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

4. The controller shall document any personal data breaches referred to in paragraphs 1 **and 2**, comprising the facts surrounding the breach, its effects and the remedial action taken[236].This documentation must enable the supervisory authority to verify compliance with this Article. **(…)**.

5. **(…).**

[6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[237]]

---

236 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.

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

Article 32

Communication of a personal data breach to the data subject[238]

1. When the personal data breach is likely to **severely** affect the rights and freedoms of the data subject[239], the controller shall (…)[240] communicate[241] 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[242] the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (f) of Article 31(3).

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

   a. the controller (…)[243] has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, in particular those that[244] render the data unintelligible to any person who is not authorised to access it, such as encryption or the use of pseudonymous data[245] [246]; or

---

238 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.

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

240 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'

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

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

243 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.

244 BE proposed 'have the purpose'.

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

b. the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer **likely to be severely affected**; or

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

d. it would adversely affect a substantial public interest.

4. **(…)**.

5. **(…).**

[6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[247]]

246 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.

247 BE, CZ, DK, DE, ES, PL and UK pleaded for the deletion of paragraph6.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment [248]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific[249] risks for the rights and freedoms of data subjects[250], the controller [or processor[251]] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. **(…)**[252].

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

   (a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on automated processing and on which decisions[253] are based that produce legal effects concerning (…) data subjects or **severely** affect data subjects[254];

---

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

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

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

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

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

253 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.

254 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).

(b) **data revealing** racial or ethnic origin**, political opinions, religion or philosphical beliefs, trade-union membership, and the processing of genetic data or data concerning health or** sex life **or criminal convictions and offences or related security measures**, where the data are processed for taking (…) decisions regarding specific individuals on a large scale[255];

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (…)on a large scale[256];

(d) personal data in large scale processing systems containing genetic data or biometric data[257];

(e) other operations where (…) the competent supervisory authority considers that the processing is likely to present specific risks for the **(…)** rights and freedoms of data subjects[258].

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.[259]

---

255 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..

256 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'.

257 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'.

258 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.

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

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. [260]

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[261], safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[262], taking into account the rights and legitimate interests of data subjects and other persons concerned[263].

4. (…)[264]

5. Where a controller is a public authority or body[265] and where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[266].

6. **(…)**

7. **(…).**

---

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

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

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

263 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.'

264 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.

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

266 IT scrutiny reservation. 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.

Article 34

Prior (…) consultation[267]

1. (…).

2. The controller [or processor[268]] 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[269].

(…)

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[270] (…) make appropriate **proposals** to the data controller or processor[271]. 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[272].

---

267 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.

268 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.

269 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.

270 IT reservation on 6-weeks period.

271 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.

272 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

(…)

4. (…)

5. (…)[273]

6. **When consulting the supervisory authority pursuant to paragraph 2,** the controller or processor[274] 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 **(…)**.[275].

7. Member States shall consult the supervisory authority during the preparation[276] of **proposals for** (…) legislative or regulatory measures which provide for the processing of personal data and which may **severely** affect categories of data subjects by virtue of the nature, scope or purposes of such processing (…).

7a. Notwithstanding paragraph 2, Member States may consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[277].

---

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.

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

274 BE was opposed to mentioning the processor here.

275 DE thought this paragraph should be deleted.

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

277 See also recital 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. For instance, Union or Member State law could provide that the processing of such data requires prior authorisation of the supervisory authority. Those safeguards also include 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

8. (…).

9. (…)

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller or the processor may, or where required by Union or Member State law shall,[278] designate a data protection officer (…)[279].

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

3. Where the controller or the processor is a public authority or body[280], a single data protection officer may be designated for several (…) such authorities or bodies, taking account of their organisational structure and size.

4. (…).

5. The (…) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37[281]**.** (…).

---

treatment or interventions provided.' (8004/13). BE proposed the following paragraph: 'Notwithstanding paragraph 2, Member States may submit by law the processing of personal data by public or private institution which executes a task of public interest, such as the contribution to the application of social security or to the execution of public health to the prior autorisation'.

278 Made optional further to decision by the Council. 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. AT scrutiny reservation. COM reservation on optional nature and deletion of points a) to c). UK thinks paragraphs 5 to 8 could be deleted

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

280 SK scrutiny reservation on this terminology.

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

6. (…).

7. (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her **tasks pursuant to Article 37**[282].

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

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

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

11. (…).

Article 36

Position of the data protection officer[283]

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

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

---

282 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.

283 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.

3. The controller or processor shall ensure that the data protection officer **can** act in an independant manner with respect to the performance of his or her tasks[284] and does not receive any instructions regarding the exercise of these tasks. The data protection officer shall directly report to the highest management level of the controller or the processor[285]**.**

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[286].

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer **(…)** with the following tasks:

   (a) to inform and advise the controller or the processor **and the employees who are processing personal data** of their obligations pursuant to this Regulation **(…);**

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

285 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.

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

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

(c) (…);

(d) (…);

(e) (…);

(f) (…)[287];

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

(h) to act as the contact point for the supervisory authority on issues related to the processing **of personal data**, including the prior consulation referred to in Article 34, and **consult, as appropriate, on any other matter**[288].

2. (….)[289].

---

287 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).

288 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.

289 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 .'

SECTION 5

CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct [290][291]

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

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

(a) fair and transparent data processing;

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

(b) the collection of data;

(ba) the use of pseudonymous data;

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

---

290 DK, FI, SK and PL scrutiny reservation. 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.

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

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

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

(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;

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

(f) transfer of data to third countries or international organisations[292].

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.

(…)[293]

2. Associations and other bodies referred to in paragraph 1a which intend to draw up a code of conduct, or to amend or extend an existing code, **shall** submit it to the supervisory authority which is competent pursuant to Article 51. **The supervisory authority may give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.**

2a. Where the code of conduct **relates to processing activities in several Member States, the supervisory authority** shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which may give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation**. (…).**

3. Where the opinion referred to in paragraph 2a confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, the European Data

---

292 NL queried whether this also covered the transfer to processors in 3rd countries.

293 See recital 76a.

Protection Board shall submit its opinion to the Commission **and shall register the code and publish details of it**[294].

[294] DE, IE, ES, PT also remarked that the DPAs should be involved. ES thought that the Commission need not necessarily be involved.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union[295]. 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[296].

Article 38a

Monitoring and enforcement of codes of conduct

1. Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 shall be carried out by an independent body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

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

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

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

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

---

295 FR scrutiny reservation regarding the legal status of such approved codes of conduct and in particular their binding nature.

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

d. **it can demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.**

3. **The competent supervisory authority shall submit the draft criteria for accreditation of the body referred to in paragraph 1 to the European Data Protection Board under the procedure referred to in Article 57.**

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

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

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

Article 39

Certification[297]

1. (…) The Member States, the European Data Protection Board and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks for procedures and products, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. **The specific needs of micro, small and medium-sized enterprises shall be taken into account.**

---

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

2. A certificate may enable the controller **or processor** to demonstrate compliance with **their** obligations under this Regulation, in particular the requirements set out in Articles 23**, 26** 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 and is without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.

4. The controller **or processor** which submits its processing to the certification mechanism shall provide the body referred to in Article 39a (1) with all information and access to its processing activities which are necessary to conduct the certification procedure. Where the processing concerns processing operations referred to in Article 33(2), the controller **[or processor]** shall provide the data protection impact assessment to the body. **The body may request the controller or processor to carry out a data protection impact assessment pursuant to Article 33 in order to support the certification process**.

5. The certification issued to a controller **or processor** 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[298]

1. **Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, t**he 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.

[298] DK, EE, FR and IT scrutiny reservation.

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

a. **it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;**

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

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

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

3. *The supervisory authorities shall submit the draft criteria for the accredition of the body referred to in paragraph 1 to the European Data Protection Board under the procedure referred to in Article 57.*

4. The body referred to in paragraph 1 shall be **responsible** for the proper assessment leading to the certification, without prejudice to the responsibility of the controller **or processor** for compliance with this Regulation.

4a. **Without prejudice to the provisions of Chapter VIII, the body referred to in paragraph 1 may, subject to adequate safeguards, in cases of inappropriate use of the certification or where the requirements of the certification are not, or no longer, met by the controller or processor, withdraw the certification.**

5. The body referred to in paragraph 1 shall **provide** the **competent** supervisory authority **with the details of** certifications issued and withdrawn and the reasons for withdrawing the certification.

6. The criteria for certification and the certification details shall be made public by the supervisory authority in an easily accessible form.

6a. **The competent supervisory authority shall revoke the accredition of a body referred to in paragraph 1 if the conditions for accredition are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.**

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including conditions for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised 'European Data Protection Seal' within the Union and in third countries].

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)[299].

_____

[299] DE pleaded in favour of deleting the last two paragraphs.