Council of the European Union

Brussels, 3 June 2015
(OR. en)

9281/15

**Interinstitutional File:**
**2012/0011 (COD)**

**LIMITE**

**DATAPROTECT 91**
**JAI 384**
**MI 350**
**DIGIT 44**
**DAPIX 85**
**FREMP 119**
**COMIX 243**
**CODEC 780**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Permanent Representatives Committee |
| No. prev. doc.: | 9398/15 |
| 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) |

In annex appears a consolidated version of the General Data Protection Regulation as it stands after the meeting of Justice and Home Affairs Counsellors on 1 June 2015.

With a view to preparing a text for a General approach which obtains the required majority in Council on 15/16 June 2015, the Presidency prepared new compromise suggestions. All changes made to the original Commission proposal are underlined; where text has been deleted, this is indicated by (…). Where existing text has been moved, this text is indicated in *italics*. Changes compared to document 9398/15 are marked in **bold**. The comments of delegations are reflected in the footnotes.

Main outstanding issues

The Presidency invites the Permanent Representatives Committee to focus the discussion on the following three main outstanding issues.

**Scope** - Article 2(2)(e), Article 21(1)(b), recital (16)

The delimitation of the scope of the two instruments in the package the General Data Protection Regulation and the Data Protection Directive. The main concern of delegations has been to ensure that the police can use only one single instrument in their work when processing personal data. The scope as initially proposed by the Commission linked the scope of the Directive to criminal offences. For many delegations that was too narrow. The police could encounter difficulties when dealing with separate rules on processing of personal data in a situation when police activities are not investigating of crimes, but other tasks in order to prevent threats to public security, for example when providing order on demonstrations.

The scope as set out in the texts relates - in addition to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences - also to the safeguarding against and the prevention of threats to public security. In the recitals to the Directive examples are set out when the Directive would be applicable and what should be excluded from its scope.

*Question 1 Can the Permanent Representatives Committee endorse the Presidency suggestion for the scope of the General Data Protection Regulation?*

**Lawfulness of processing** - Article 6, recital (40), Article 19(1)

In March 2015, the Council reached a Partial General Approach on Article 6 and recital (40) on the basis of the understanding that these concern cross-cutting issues that needed to be addressed at a later occasion. Against that background, further discussions were pursued in Council's preparatory bodies.

An essential issue concerned Article 6(4). The first sentence of Article 6(4) provides that, where the purpose of further processing is incompatible with the one for which the personal data have been collected by the same controller, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1 (consent, contract, legal obligation, protection of vital interests, task of public interest) . The second sentence of Article 6(4) provides that further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party is lawful if these interests would override the interests of the data subject. This provision raised the question whether, as a result of such further processing for incompatible purposes, the level of data protection rights would not go below the level currently ensured by Directive 95/46. Furthermore, some delegations expressed concerns that Article 6(4) could tip the balance in favour of the data controller to the detriment of the data subject.

As regards the question on the level of data protection rights, the Presidency suggests to maintain in the General Approach the agreement reached on the Partial General Approach and assess in the negotiations between the Council and the European Parliament whether modifications are needed. Furthermore, the Presidency suggests to strengthen the position of the data subject in relevant cases of further processing on the basis of Article 6(4), by enhancing in Article 19(1) his or her possibilities to make use of the right to object to processing of personal data concerning him or her. Data subjects would then have the right to object in 4 situations, two of which concern initial processing and two further processing:

1. processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e);
2. processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party 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 (Article 6(1)(f);
3. <u>further</u> processing by the same controller for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (first sentence of Article 6(4) in conjunction with point (e) of Article 6(1));

4. further processing carried out by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject ( second sentence of Article 6(4)).

*Question 2. Can the Permanent Representatives Committee endorse maintaining the Partial General Approach of March 2015 while supplementing it with a strengthened right to object in Article 19(1)?*

**Right to compensation and liability** - Article 77 and recitals (112), (113a), (118), (118b)

Article 77 deals with the conditions under which a controller and/or processor can be held liable for con-compliance with the Regulation. Paragraph 1 set out that the data subject can receive compensation from both the controller and the processor. Paragraph 2 now refers to **the** processing and not to *its* processing to underline that it is the main responsible for the processing. The processor's more limited liability is set out in the second sentence. Paragraph 3 has been modified to clarify that the controller or processor could be exempted from liability if it is not in any way liable for the whole damage. The language is both paragraphs 2 and 3 has been made consistent with the wording in the other paragraphs.

*Question 3 Can the Permanent Representatives Committee endorse the Presidency suggestion on liability for and compensation of damage suffered as a consequence of non-compliance with the General data Protection Regulation?*

Other issues

In addition to these main issues, the Presidency makes also some new suggestions on other issues in the text which appears in annex:

– recital (52)
– Recital (60c), recital (66a)
– Recital 81

- Recital 112
- Recital 113a
- Recital 118
- Recital 118b
- recital (132)
- recital (135)
- unauthorized reversal of pseudonymisation - Article 28(4)(b), Article 31(1), Article 32(1), Article 33(1), recital (60a), recital (67)
- 76(2)
- 77(2)(3)(4)
- Article 79(2a)(i)

*Question 4. Can the Permanent Representatives Committee endorse the text for a General approach of the General data Protection Regulation, including the other issues?*

**ANNEX**

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[1],

After consulting the European Data Protection Supervisor[2],

Acting in accordance with the ordinary legislative procedure,

[1] OJ C, p. . .
[2] OJ C p. .

Whereas:

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

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

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

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

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

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

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

6) These developments require (…) a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.[4]

6a) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for the coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of the Regulation in their respective national law.

[4] DE proposal to add such wording to recital "As far as the General Data Protection Regulation provides for legislative measures of the Member States for specifications (e.g. Article. 1 paragraph 2a, Article 6 paragraph 3, Article 83) and restrictions (e.g. Article 21) the Member States may, in their national law, repeat the wording of the various rights and provisions under the General Data Protection Regulation if the national legislators find this to be necessary in the interest of those the rules apply to."

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

8) In order to ensure a consistent and high level of protection of individuals and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation,[5] for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC Member States have several sector specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules. Within this margin of manoeuvre sector-specific laws that Member States have issued implementing Directive 95/46/EC should be able to be upheld.

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

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

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

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

[6] SI: reservation.

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

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

14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, (…) nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union. [7]

14a)[8] Regulation (EC) No 45/2001[9] applies to the processing of personal data by the Union institutions, bodies, offices and agencies[10]. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.

---

7 NL prefers not to have specific references to provisions in the Treaty.

8 BE, supported by DE and IE, suggested to delete recital (14a).
PL expressed support for the EP amendment on recital(14) of the Commission proposal.
CZ proposes that recital 14a includes explicit reference to the already stated intention of the Commission to propose an overhaul of Regulation 45/2001/EC to harmonize it with this Regulation in time for it to enter into force at the same moment. It could be said then that while the updated Regulation 45/2001/EC will provide for the same level of data protection, it will be tailored better to the specificities of EU institutions.
Cion referred to its statement made at the JHA Council in June 2013 in which it has indicated its intention to align Regulation 45/2001 after agreement on the GDPR.

9 OJ L 8, 12.1.2001, p. 1.

10 FR, SI: scrutiny reservation about applicable rules for EU agencies.

15) This Regulation should not apply to processing of personal data by a natural person[11] in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities.[12] However, this Regulation should (…) apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences**,** the execution of criminal penalties **~~and~~ or the safeguarding against** and the prevention of threats to public security[13], and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY). **Member States may entrust competent authorities within the meaning of Directive XX/YYY with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of the this Regulation.**

---

11 **SK suggested to insert "exclusively"**

12 DE queried whether it should be clarified in the regulation whether the household exemption of Article 2(2)(c) applies regardless of the number of data subjects affected. In this context, ES and IT referred to the discussions in the Article 29 working group. BE reacted that the rules of the GDPR are too complicated for individual persons. IE, UK expressed doubts about trying to specify the household exemption.

13 Cion reservation.
The exact wording of the recital and of Article 2(2)(e) will need to be aligned to that of the data protection Directive still under discussion.

When processing of personal data by (...) private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

16a) *While this Regulation applies also to the activities of courts* and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. *The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity*, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including its decision-making. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.

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

18) (…)

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

20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.

21) The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union. In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes. [14].

23aa) The principles of data protection should not apply to data of deceased persons. The national law of a Member State may provide for rules regarding the processing of data of deceased persons**.**

[14] The question of the application of the Regulation to deceased persons may need to be revisited in the future.

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

23b) (…)

23c) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented, taking into account the respective data processing and ensuring that additional information for attributing the personal data to a specific data subject is kept separately. The controller who processes the data shall also refer to authorised persons within the same controller. In such case however the controller shall make sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data[15].

24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not (…) be considered as personal data if they do not identify an individual or make an individual identifiable[16].

[15] COM, IE, IT, AT, SE, UK reservation and FR scrutiny reservation on two last sentences.
[16] DE reservation. AT and SI thought the last sentence of the recital should be deleted.

25) Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, including[17] electronic, oral statement or, if required by specific circumstances, by any other clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application[18]. In such cases it is sufficient that the data subject receives the information needed to give freely specific and informed consent when starting to use the service. (…). Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided[19].

---

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

18 PL and AT reservation.

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

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.

25aa) It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects can give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research[20]. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose[21].

26) Personal data concerning health should include (…) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject[22]; including information about the registration of the individual for the provision of health services (…); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (…) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (…) or any information on for example a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

---

20 FR, AT and COM scrutiny reservation.

21 AT, CZ, PL, SI and FR scrutiny reservation; IT and COM reservation.

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

27) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes (…) and means of processing through stable arrangements. This criterion should not depend on whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered as concerned supervisory authorities when the draft decision concerns only the controller.

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

28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. A central undertaking which controls[23] the processing of personal data in undertakings affiliated to it forms together with these undertakings an entity which may be treated as "group of undertakings[24].

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. (…)[25]. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child[26].

---

23 ES suggestion, in line with the definition of group of undertakings.

24 FI proposal supported by NL.
SI reservation.

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

26 CZ and AT reservation.

30) Any processing of personal data should be lawful and fair. (…). It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data.[27] The data should be adequate and relevant (…) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (…). Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means[28]. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.

---

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

**28** UK reservation: this was too burdensome.

31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

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

32) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that, and the extent to which, consent is given. A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and its content should not be unusual within the overall context. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.

33) (…)

34) In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent[29].

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

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

[29] COM, DE, DK, IE, NL and FR, SE reservation. CZ thought the wording should be more generic. IE suggested replacing the final part of the sentence with the following: "... or if the performance of a contract is made dependant on consent to a different data processing operation despite this not being necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without such consent."

36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a (…) basis in Union law or in the national law of a Member State. (…). It should be also for Union or national law to determine the purpose of the processing. Furthermore, this (…) basis could specify the general conditions of the Regulation governing the lawfulness of data processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.

It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.

37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person. (…). Some types of *data processing may serve both important grounds of public interest and the vital interests of the data subject as, for instance when processing is necessary for* humanitarian purposes, including for *monitoring epidemic and its spread or in situations of humanitarian emergencies, in particular in situations of natural disasters*[30].

[30] CZ, FR, SE and PL thought the entire recital was superfluous.

38) The legitimate interests of a controller including of a controller to which the data may be disclosed or of a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller[31]. (…) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. (…)

38a) Controllers that are part of a group of undertakings or institution affiliated to a central body may have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes**,** including the processing of clients' or employees' personal data. The general principles for the transfer of personal data**,** within a group of undertakings, to an undertaking located in a third country (…) remain unaffected.[32]

**31** HU scrutiny reservation.
**32** FR reservation.

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

40) [33]The processing of personal data for other purposes than the purposes for which the data have been initially collected should be only allowed where the processing is compatible with those purposes for which the data have been initially collected. In such case no separate legal basis is required other than the one which allowed the collection of the data[34]. (…) If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law or Member State law may determine and specify the tasks and purposes for which the further processing shall be regarded as lawful. The further processing (…) for archiving purposes in the public interest or, statistical, scientific or historical (…) purposes (…) or in view of future dispute resolution[35] should be considered as compatible lawful processing operations. The legal basis provided by Union or Member State law for the collection and processing of personal data may also provide a legal basis for further processing for other purposes if these purposes are in line with the assigned task and the controller is entitled legally to collect the data for these other purposes[36].
In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account inter alia 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 the existence of appropriate safeguards in both the original and intended processing operations. Where the intended other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. (…).

---

33 **AT reservation**
**FR scrutiny reservation**

34 Cion reservation.
DE suggested to replace other than the one which allowed the collection of the data " but as long as the original legal basis covers as well the processing for the further purpose.

35 ES pointed out the text of Article 6 had not been modified regarding dispute resolution.

36 FR, IT and UK scrutiny reservation.

In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes and on his or her rights (…) including the right to object, should be ensured. (…). Indicating possible criminal acts or threats to public security by the controller and transmitting these data to a competent authority should be regarded as being in the legitimate interest pursued by the controller[37]. However such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.[38]

41) Personal data which are, by their nature, particularly sensitive (…) in relation to fundamental rights and freedoms, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation[39]for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly be provided inter alia where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

---

**37** AT, PL and COM reservation.

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

**39** AT scrutiny reservation.

Special categories of personal data may also be processed where the data have manifestly been made public or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject.

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

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

This may be done for health purposes, including public health (…) and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving in the public interest or historical, statistical and scientific (…) purposes.

A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.

42a) *Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health or social care services* and systems including the processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, *and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health. Therefore this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy (…). Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (…)*[40].

[40] Moved from recital 122.

42b) *The processing of special categories personal data* (…) *may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to for suitable and specific measures so as to protect the rights and freedoms of individuals. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies*[41].

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

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

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

[41] Moved from recital 123.

46) [42]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 and, additionally, where appropriate, visualisation is used. This information could be provided also 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 without undue delay and at the latest within a fixed deadline of one month and give reasons where the controller does not intend to comply with the data subject's request.

[42] DE suggestion (8089/15) partly taken over.

However, if requests are manifestly unfounded or excessive[43] such as when the data subject unreasonably and[44] repetitiously requests information or where the data subject abuses its right to receive information for example by providing false or misleading information when making the request, the controller could[45] refuse to act on the request. [46]

48) [47]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.

---

43 Cion suggestion. As in Article 12(4).

44 CZ suggested or instead of "and".

45 PT suggested instead "may".

46 AT suggested to delete the last sentence as repetitiously requesting information must not as such be considered that the request is manifestly unfounded. Alternatively, AT suggested"However, if requests are manifestly unfounded such as when the data subject repetitiously requests information *despite complete and correct information or despite properly substantiated denial of information or well-founded restriction of information by the controller* ~~or where the data subject abuses its right to receive information for example by providing false or misleading information when making the request~~, the controller could refuse to act on the request."
AT: scrutiny reservation on "abuses its right".

47 AT suggested "shall" instead of "should" throughout recital (48).

49) [48]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 controller intends to process the data for a purpose other than the one for which the data were collected the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information[49]. Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner.

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

---

48 AT suggested "shall" instead of "should" throughout the recital.

49 NL suggested to insert "in an appropriate manner" with a view to alleviating concerns of business. IE considered this sentence burdensome, in particular in case the other purpose is compatible with the initial purpose.

51) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. *This includes the right for individuals to have access to their [50]personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.* Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, where possible for what period, which recipients receive the data, what is the logic involved in any automatic data processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates.

[50] FR suggested to insert "login data and to their".

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. (…) Identification should include the digital identification of a data subject, for example through **authentication mechanism such as the same credentials, used by the data subject to log-into the on-line service offered by the data controller ~~a log-in or an e-mail address~~**[51]. A controller should not retain personal data for the sole purpose of being able to react to potential requests.[52]

---

[51] Presidency suggestion to ensure identification in digital era amended according to BE proposal.
CZ, SI: reservation on added phrase.

[52] **Presidency sugegstion taking into account the sugegstions of RO and BE. RO suggested:** "*~~for example through a log-in or an e-mail address~~*" with „***for example through the same credentials (username or e-mail address and password or any other combination of credentials used to log into an on-line service ) used by the data subject to log-into the on-line service offered by the data controller*****". BE suggested: "**Identification should include the digital identification of **a** data subject, for example **through an authentication mechanism,** such as log-in ~~or an e-mail address,"~~

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 or with Union or Member State law to which the controller is subject. 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[53]. The data subject should be able to exercise this right notwithstanding the fact that he or she is no longer a child. However, the further retention of the data should be lawful[54] where it is necessary for *exercising the right of freedom of expression* and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, *for reasons of public interest in the area of public health,* for archiving purposes in the public interest, for historical, statistical and scientific (…) purposes or for the establishment, exercise or defence of legal claims.[55]

---

53 Inspired by FR suggestion, supported by HU, SI, to strengthen the rights of children as follows: This right should be exercised notwithstanding the fact that the data subject is no longer a child.

54 DE suggestion.

55 NL considered that recital (53a) could be deleted as it is covered by recital (54a). PL made a suggestion for an alternative text of recital (53a) (7586/15 REV1).

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 who are processing such data **(…)** to erase any links to, or copies or replications of that personal data.

To ensure the above[56] mentioned information, the controller should take (…) reasonable steps, taking into account available technology and the means available to the controller, including technical measures, in relation to data for the publication of which the controller is responsible. (…).

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

55) To further strengthen the control over their own data (…), where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive the personal data concerning him or her[57], which he or she has provided to a controller, in a structured and commonly used and machine-readable format and transmit it to another controller.

This right should apply where the data subject provided the personal data based on his or her consent or in the performance of a contract. It should not apply where processing is based on another legal ground other than consent or contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.

---

**56** DE suggested "the above" instead of "this".

**57** **DE, FR Cion, wanted to re-insert in Article 18(2) and in recital (55) the phrase "and any other information" considering that not having this phrase would decrease the scope of data portability too much.**
**Cion: scrutiny reservation.**

The data subject's right to transmit personal data does not create an obligation for the controllers to adopt or maintain data processing systems which are technically compatible.[58]

Where, in a certain set of personal data, more than one data subject is concerned, the right to transmit the data should be without prejudice to the requirements on the lawfulness of the processing of personal data related to another data subject in accordance with this Regulation. [59]This right should also not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should in particular not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. (…)

56) [60]In cases where personal data might lawfully be processed (…) because 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 or on grounds of (…) the legitimate interests of a controller or a third party, any data subject should nevertheless be entitled to object to the processing of any data relating to their particular situation. It should be for the controller to demonstrate that their compelling legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

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

---

58 FI proposal.
**AT and Cion scrutiny reservation.**

59 FR suggested to delete the first sentence of this subparagraph. In reaction, Pres explained that recital 55 was narrower than right to access because it concerned right to data portability.

60 Presidency suggestion to bring recital (56) in line with Article 19(1).

58) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her **(…)** which is based solely on automated processing, *which produces legal effects concerning him or her* or significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' consisting in any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements as long as it produces legal effects concerning him or her or significantly affects him or her[61]. However, decision making based on such processing, including profiling, should be allowed when authorised by Union or Member State law to which the controller is subject, including for fraud and tax evasion monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention, to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision. In order 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, the controller should use adequate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure in particular that factors which result in data inaccuracies are corrected and the risk of errors is minimized, secure personal data in a way which takes account of the potential risks involved for the interests and rights of the data subject[62] and which prevents inter alia discriminatory effects against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, sexual orientation or that result in measures having such effect[63]. Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.

---

**61** UK suggested to insert "in an adverse manner". In reaction, Cion indicated this would lower data protection standards.
AT reservation on "as long as it produces legal effects concerning him or her or significantly affects him or her".

**62** Further to DE proposal. IE expressed doubts about the before last sentence.

**63** UK considered Regulation not the appropriate place to refer to anti-discrimination measures.

58a) Profiling as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.[64]

59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection**,** public health and humanitarian purposes, such as the performance of a task incumbent upon the International Red Cross and Red Crescent Movement **(…)**.[65] 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.

59a*)* Nothing in this Regulation should derogate from (…) the privilege of non-disclosure of confidential information of the International Committee of the Red Cross under international law, which shall be applicable in judicial and administrative proceedings. (…).

---

[64] DE suggested in recital (59) to delete "public" in "…the keeping of public registers".

[65] **AT opposed explicit mentioning of International Red Cross and Red Crescent Movement in recitals (59), (59a) and (87).**

60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation (…). These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.

60a) Such risks, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, **unauthorized reversal of pseudonymisation**, or any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects; (…).

60b) *The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a high risk. A high risk is a particular*[66] *risk of prejudice to the rights and freedoms of individuals* (…).

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

60c) Guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller ~~**or processor**~~[67], especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk for the rights and freedoms of individuals and indicate what measures may be sufficient in such cases to address such risk. (…)

61) The protection of the rights and freedoms of individuals with regard to the processing of personal data require that appropriate technical and organisational measures are taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

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

---

[67] **AT, BE, ES scrutiny reservation**

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of their behaviour in the Union, (…) the controller should designate a representative, unless (…) *the processing it carries out is* occasional and unlikely *to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing* or the controller is a public authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance by the controller.

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

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

64) (…)

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

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the (…) risks inherent to the processing and implement measures to mitigate those risk. These measures should ensure an appropriate level of security, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risk and the nature of the personal data to be protected. (…). In assessing data security risk, consideration should be given to the risk**s** that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller **or** the processor[68] should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

[68] AT: scrutiny reservation

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

68) (…) It must be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject (…). The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

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

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

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, *context* and purposes (…). Such types of processing operations may be those which, in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing[69].

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

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

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

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

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

74) Where a data protection impact assessment indicates that the processing would, despite the envisaged safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of individuals (…), and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted, prior to the start of the processing activities. Such high (…) risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of (…) damage or (…) interference with the rights and freedoms of the data subject. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of individuals.

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

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

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

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

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

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

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or[70] another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects[71].

---

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

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

80) The Commission may (…) decide with effect for the entire Union that certain third countries, or a territory or a specified sector, such as the private sector or one or more specific economic sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations, which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of a third country or of a territory or of a specified sector within a third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. **The third country should offer guarantees that ensure an adequate level of protection in particular when data are processed in one or several specific sectors. In particular, the third country should ensure effective data protection supervision and should provide for cooperation mechanisms with the European data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.**[72]

[72] **The Presidency suggests this wording to take into account the DE request for Article 41(2)(c).**

81a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol *should be taken into account*. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations[73].

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

82) The Commission may (…) recognise that a third country, or a territory or a specified sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

---

[73] DE, supported by NL, proposed that the list of checks in Article 42(2) should include a new component consisting of the participation of third states or international organisations in international data-protection systems (e.g. APEC and ECOWAS). According to the position of DE, although those systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards.

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or ad hoc contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. They should relate in particular to compliance with the general principles relating to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.

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

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

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

87) These rules should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange (….) between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, for example in case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport (…) .A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent.[74] In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation, such as a National Society of the Red Cross **(…)** or to the ICRC of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent upon the International Red Cross and Red Crescent Movement under the Geneva Conventions and/or to work for the faithful application of international humanitarian law applicable in armed conflicts **c**ould be considered as necessary for an important reason of public interest or being in the vital interest of the data subject.

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

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms of natural persons with respect to processing of their personal data. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

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

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

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

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

92a) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subjected to control or monitoring mechanism regarding their financial expenditure. Neither does it imply that supervisory authorities cannot be subjected to judicial review.

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

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

95) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament and/or the government or the head of State of the Member State or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. (…).

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

96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, this Regulation should oblige and empower the supervisory authorities to co-operate with each other and the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

97) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities that are concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority to which such complaint has been lodged should also be a concerned supervisory authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection[75].

97a) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the concerned supervisory authorities in the decision-making process. In cases where the decisions is to reject the complaint by the data subject in whole or in part that decision should be adopted by the supervisory authority at which the complaint has been lodged.

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

97b) The decision should be agreed jointly by the lead supervisory authority and the concerned supervisory authorities and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

97c) Each supervisory authority (…) not acting as lead supervisory authority should be competent to deal with (…) local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involving only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay on this matter. After being informed, the lead supervisory authority should decide, whether it will deal with the case within the one-stop-shop mechanism or whether the supervisory authority which informed it should deal with the case at local level. When deciding whether it will deal with the case, the lead supervisory authority should take into account, whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it, in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to deal with the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in the one-stop-shop mechanism.

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

99) (…)

100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, particularly in cases of complaints from individuals, and without prejudice to the powers of prosecutorial authorities under national law, to bring infringements of this Regulation to the attention of the judicial authorities and/or engage in legal proceedings. Such powers should also include the power to forbid the processing on which the authority is consulted. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities (…) should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in national procedural law, such as the requirement to obtain a prior judicial authorisation.

Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to national procedural law. The adoption of such legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

101) (…).

101a) Where the supervisory authority to which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

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

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

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

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

105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities (…) should be established. This mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States (…). It should also apply where any *concerned* supervisory authority or the Commission[76] requests that such matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

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

106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a (…) majority of its members so decides or if so requested by any *concerned* supervisory authority or the Commission. The European Data Protection Board should also be empowered to adopt legally binding decisions in case of disputes between supervisory authorities. For that purposes it should issue, in principle with a two-third majority of its members, legally binding decisions in clearly defined cases where there are conflicting views among supervisory authorities in particular in the cooperation mechanism between the lead supervisory authority and *concerned* supervisory authorities on the merits of the case, notably whether there is an infringement of this Regulation or not.

107) (…)

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

109) The application of this mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and *concerned* supervisory authorities should be applied and mutual assistance and joint operations might be carried out between the *concerned* supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

110) In order to promote the consistent application of this Regulation, the European Data Protection Board should be set up as an independent body of the Union. To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State or his or her representative (…). The Commission *and the European Data Protection Supervisor* should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

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

111) Every data subject should have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence , and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication. [77]

112) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects. Member States may provide that **s**uch a body, organisation or association should have the right to lodge, independently of a data subject's mandate, **in such Member State** a complaint-and/or have the right to an effective judicial remedy where it has reasons to consider that (…) the rights of a data subject's right have been infringed as a result of the processing of personal data which are not in compliance with this Regulation. This body, organisation or association **~~does~~ may** not **be allowed ~~have the right~~** to claim compensation on a data subject's behalf.[78]

---

**77** FI suggested to insert a footnote to accommodate its concern that inaction on behalf of an authority was unknown in their legal system, with the following wording: 'In a case of inaction by the supervisory authority under art. 74(2), an effective judicial remedy may be provided by courts, tribunals or other kind of judicial bodies, such as the Chancellor of Justice or the Parliamentary Ombudsman, as far as such remedy will factually lead to appropriate measures.'

**78** NL suggestion.

113) Any natural or legal person has the right to bring an action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union (the "Court of Justice") under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the concerned supervisory authorities who wish to challenge them, have to bring action within two months of their notification to them, in accordance with Article 263 TFEU. Where decisions of the European Data Protection Board are of direct and individual concern to a controller, processor or the complainant, the latter may bring an action for annulment against those decisions and they should do so within two months of their publication on the website of the European Data Protection Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning this person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints[79]. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation.

[79] GR reservation.

Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[80], whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the European Data Protection Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.

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

114) (…)

115) (…)

**80** Case C-314/85.

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

117) (…).[81]

118) Any damage which a person may suffer as a result of ~~**unlawful**~~ **a** processing **that it not in compliance with this Regulation** should be compensated by the controller or processor, who should be exempted from liability if they prove that they are not **in any way** responsible for the damage. ~~**in particular where he establishes fault on the part of the data subject or in case of force majeure.**~~ The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law[82]. (...)
**When reference is made to a processing that is not in compliance with this Regulation it also covers processing that is not in compliance with delegated and implementing acts adopted in accordance with this Regulation and national law implementing this Regulation.**

Where controllers or processors are involved in the same processing they may be joined to the same proceedings, in accordance with national law. Where controllers and processors involved in the same processing have not been joined to the proceedings or this is not permitted under national law, any controller or processor who has been held liable, may subsequently institute recourse proceedings against other controllers or processors involved in the same processing. In such case the court may take into account whether each controller's controller`s or processor's breach of this Regulation caused all of the damage.[83]

---

**81** FR suggested to insert a footnote on contractual clauses as follows: 'Any contractual clause which is not compliant with the right to an effective judicial remedy against a controller or processor, and in particular with the right of the data subject to bring proceedings before the courts of the Member State of its habitual residence shall be null and void.'

**82** COM scrutiny reservation.

**83** **EL wanted to delete the last sentence.**

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

118b) In order to strengthen the enforcement of the rules of this Regulation, penalties and administrative fines[84] may be imposed for any infringement of the Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute an disproportionate burden to a natural person, a reprimand may be issued instead of a fines. Due regard should however be given to the **nature, gravity and duration of the infringement,** the intentional character of the infringement, actions taken to mitigate the damage suffered , degree of responsibility or any relevant *previous infringements*, **the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor** [85] The imposition of penalties and administrative fines should be subject to adequate procedural safeguards in conformity with general principles of Union law and the Charter of Fundamental Rights, including effective judicial protection and due process. Where the national law of a Member State does not provide for administrative fines, such Member State may abstain from providing administrative fines for infringements of this Regulation that are already subject to criminal sanctions in their national law ensuring that these criminal sanctions are effective, proportionate and dissuasive**,** taking into account the level of administrative fines provided for in this Regulation.

---

**84** DK reservation on the introduction of administrative fines in the text as administrative fines – irrespective of their level – raise constitutional concerns.

**85** Further to FI proposal. FR wanted to delete the text of this suggestion.

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

120) In order to strengthen and harmonise administrative penalties against infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate offences, the upper limit and criteria for fixing the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the breach and of its consequences and the measures taken to ensure compliance with the obligations under the Regulation and to prevent or mitigate the consequences of the infringement. Where the fines are imposed on persons that are not a commercial undertaking, the supervisory authority should take account of the general level of income in the Member State in considering the appropriate amount of fine[86]. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other sanctions under the Regulation.

120a) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the Regulation[87], Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties (criminal or administrative) should be determined by national law.

---

**86** Further to CZ proposal. FR wanted to delete the text of the CZ suggestion.

**87** IE thought that it was not necessary to have additional conditions like 'serious' infringements.

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

121a) *This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary derogations from the rules of this regulation. The reference to public authorities and bodies should in this context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data*[88].

122) (…)[89].

123) (…)[90].

[88] Moved from recital 18.
[89] Moved to recital 42a.
[90] Moved to recital 42b.

124) National law or collective agreements (including 'works agreements')[91] may provide for *specific rules on the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace , health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*

125)[92] The processing of personal data for historical, statistical or scientific (…) purposes and for archiving purposes in the public interest (…) should, in addition to the general principles and specific rules of this Regulation, in particular as regards the conditions for lawful processing, also comply with respect other relevant legislation such as on clinical trials. The further processing of personal data for historical, statistical and scientific purposes and for archiving purposes in the public interest (…) should not be considered incompatible with the purposes for which the data are initially collected and may be processed for those purposes for a longer period than necessary for that initial purpose (…). Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements and the rights to access, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for historical, statistical or scientific purposes and for archiving purposes (…) The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.

125a)(…)[93].

---

**91** DE proposal.
**92** **AT: reservation**
**93** Moved to recitals 126c and 126d.

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

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

125b) The importance of archives for the understanding of the history and culture of Europe" and "that well-kept and accessible archives contribute to the democratic function of our societies', were underlined by Council Resolution of 6 May 2003 on archives in the Member States[94]. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons.

Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide that personal data may be further processed for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes[95].

---

**94** OJ C 113, 13.5.2003, p. 2.

**95** CZ reservation.

Codes of conduct may contribute to the proper application of this Regulation, including when personal data are processed for archiving purposes in the public interest by further specifying appropriate safeguards for the rights and freedoms of the data subject[96]. Such codes should be drafted by Member States' official archives or by the European Archives Group. Regarding international transfers of personal data included in archives, these must take place without prejudice of the applying European and national rules for the circulation of cultural goods and national treasures.

126) Where personal data are processed for scientific purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, processing of personal data for scientific purposes should include fundamental research, applied research, privately funded research[97] and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. Scientific purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures[98].

**96** CZ, DK, FI, HU, FR, MT, NL, PT, RO, SE, SI and UK scrutiny reservation.
**97** AT and SE scrutiny reservation.
**98** CZ, DK, FI, FR, HU, MT, NL, PT, SE, SI and UK scrutiny reservation.

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

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

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

126d) *The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in conformity with the statistical principles as set out in Article 338(2) of the Treaty of the Functioning of the European Union, while national statistics should also comply with national law. Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities*[99] *provides further specifications on statistical confidentiality for European statistics.*

[99] OJ L 87, 31.3.2009, p. 164–173.

127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt professional secrecy where required by Union law.

128) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. (...).

129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of **(…)**; criteria and requirements for certification mechanisms; **(…)**; **(…)**[100] It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

**100** Cion against deletion.

130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: **(…);** standard contractual clauses between controllers and processors and between processors, codes of conduct; (…) technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; adopt standard data protection clauses; formats and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules; **(…)** mutual assistance; **(…);** the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board[101]. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[102]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

[101] Cion against deletion.

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

131) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; **(…)** technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; adopt standard data protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; (…) the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board [103]given that those acts are of general scope.

132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection ~~**and relating to matters communicated by supervisory authorities under the consistency mechanism**~~, imperative grounds of urgency so require.[104]

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

---

**103** Cion against deletion.

**104** **Presidency suggestion to bring recital 132 in line with Article 41.**
**AT, FR, Cion: scrutiny reservation.**
HU considered the phrase "and relating …so require" superfluous.

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

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

136) (…)

137) (…)

138) (…)[105].

139) (…)[106]

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

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

HAVE ADOPTED THIS REGULATION:

# CHAPTER I

# GENERAL PROVISIONS

*Article 1*

***Subject matter and objectives***[107]

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

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

2a. Member States[108] may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations as provided for in Article 6(1)(c) and (e)[109] by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX[110].

---

107 DE suggested to insert new recital (48a) (8089/15).
FR suggested to insert a reference that data subjects have a right to obtain their data. FR suggested to insert "Data subjects have the right to decide upon the communication and use of their personal data within the conditions and limits set forth in the present regulation".

108 BE suggested to insert "and institutions of the European Union". DE and IE considered this suggestion worth considering. In response to queries of BE, CZ, DE, HU, NL, ES about non applicability to EU institutions Cion referred to recital (14a) and the remarks made at the JHA Council in June 2013 that the Regulation applicable to the EU Institutions would be applicable at the same time as the GDPR and the Police Directive

109 **HU asked to insert a reference to Article 9(2).**

110 AT (15768/15), HU, SI reservation. These delegations were in favour of a minimum harmonisation clause for the public sector. HU, supported by SK requested to clarify the limits of paragraph (2a).
LU reservation considering this offers too much leeway.

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data[111].

*Article 2*

***Material scope***

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system[112].

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

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

(b) by the Union institutions, bodies, offices and agencies[113]**;**

---

**111** SI scrutiny reservation.

**112** HU, supported by EE and IT, and disadvised by IE and Cion referring to the long discussions on data processed by non automated means, objected to the fact that data processing operations not covered by this phrase would be excluded from the scope of the Regulation and thought this was not compatible with the stated aim of a set of comprehensive EU data protection rules. HU therefore proposed to replace the second part by the following wording 'irrespective of the means by which personal data are processed'. Cion further argued that the text of draft regulation not implied a restriction compared to the directive currently in force which refers to filing systems.

**113** The Presidency suggests not to apply the regulation to Union institutions, bodies, offices and agencies in line with the current acquis where the rules for processing of personal data by Union institutions, bodies, offices and agencies are laid down in Regulation (EC) No 45/2001.The new EU data protection framework based on Article 16 TFEU will cover both Member States and EU institutions and bodies. The Commission intends to present the necessary proposals which will align Regulation 45/2001 with the principles and rules of the General Data Protection Regulation as agreed by the co-legislators. The Commission intends to present such proposals in a timely manner in order to ensure that the amended Regulation 45/2001 can enter into application at the same time as the General Data Protection Regulation. BE, ES and PL did not support the insertion of the EU bodies.

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

(d) by a natural person (…)[114] in the course of (…)[115] a personal or household activity;

(e) by competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences**,** the execution of criminal penalties **or the safeguarding against and the prevention of threats to public security** [116].

3. (…).

*Article 3*

***Territorial scope***

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

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

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union[117].

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

---

114 **SK suggested to insert "exclusively".**

115 AT suggested to insert "solely" or "exclusively" both in Article 2 and in recital (15) with a view to avoid lowering standards compared to the directive currently in force.

116 Cion: reservation. The exact wording of Article 2(2)(e) and the corresponding recital (16) will need to be aligned to that of the data protection Directive still under discussion.

117 UK reservation.

*Article 4*

***Definitions***

For the purposes of this Regulation:

(1) [118]'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[119] such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

(2a) (…)

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means[120], such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination (…) restriction, erasure or destruction[121];

(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future[122];

---

118 BE suggested to change the definition on the basis of recital (23).

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

120 HU suggested to delete "whether or not by automated means".

121 Suggestion of DE, FR and SK which regretted that not all elements included in the list of data processing operations of the directive currently in force are listed in the definition of processing. These delegations argued these elements were especially useful in the public sector. COM indicated that the right to have the processing restricted in certain cases was provided for in Article 17a (restriction of data processing), even though the terminology 'blocking' was not used there. The term "blocking" was not used because it has a special connotation on the Internet related to censorship. DE and FR thought the definition of Article 4(3) (erasure) should be linked to Article 17.

122 FR, RO scrutiny reservation.

(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person (…)[123].

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis[124];

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;[125]

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

---

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

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

125 CZ: delete "and means".

**126**

(7) 'recipient' means a natural or legal person, public authority, agency or any other body (…) to which the personal data are disclosed, whether a third party or not;[127] however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients[128] [129];

(8) 'the data subject's consent' means any freely-given, specific and informed (…)[130] indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

---

126 DE, DK, FR, HU, IT, LU and NL, opposed by Cion, requested the inclusion of a definition of third party.
HU suggested: 'third party' 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."
SK suggested also a definition of "third party": **´third party´ means any entity other than the data subject, the controller providing personal data or the controller's representative or his processor. Alternatively, SK could accept the HU version.**

127 Suggestion of DE, FR, LU, NL, SI and SE which 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. CZ suggested to delete "whether a third party or not".

128 AT, ES, HU, HR, NL suggested to delete the phrase "however … recipients" and DE, UK scrutiny reservation on latter part of previous text of the definition. IE insisted on keeping this phrase.
Suggestion by AT, ES, IT (supported by FR and Cion to go back to the wording of the directive currently in force), NL and UK thought it could be deleted.
HU, opposed by PL suggested: " recipient means a natural or legal person, public authority, agency or any other body to which personal data are disclosed".

129 AT suggested to insert a definition of further processing under reference to its Statement to the JHA Council in March 2015.

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

(9) 'personal data breach' means a breach of security[131] leading to the accidental or unlawful destruction[132], loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[133];

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, **(…)** which give unique information about the physiology or the health of that individual[134], resulting in particular[135] from an analysis of a biological sample from the individual in question[136];

---

131 In light of opposition CZ, IE, FR, IT, NL and Cion on deletion "of security", Presidency re-inserts this phrase.
HU suggestion: "personal security breach means a breach of the provisions of this Regulation leading to any unlawful operation or set of operations performed upon personal data such as the accidental …"

132 HU suggested ".. breach of the provisions of this regulation leading to any unlawful operation performed on personal data such as….". Cion did not support this suggestion.

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

134 AT, FI: scrutiny reservation.
DK, ES, IT, MT, NL, SE rejected the limitation to "during pre-natal development" considering that genetic data can change after birth for example as a result of a cancer treatment. DE found this phrase important.
In this context, BE referred to Recommendation 97/15 of the Council of Europe.
CZ reservation considering that genetic changes can also take place after birth, for example after a transplantation.

135 Added at the request of FR, supported by AT, EE, ES, IT and SI.

136 AT, CY, DE, FR, 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. 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 allows or confirms the[137] unique identification of that individual, such as facial images, or dactyloscopic data[138];

(12) 'data concerning health' means data related to the physical or mental health of an individual, which reveal information about his or her health status[139];

(12a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements[140];

(12b) (…)[141]

---

137 ES preferred 'allows' SI: scrutiny reservation on last part.

138 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'. ES explained that research is done to recognising persons by the way the y move or speak. CH is of the opinion that the term 'biometric data' is too broadly defined. HU suggested to specify when "facial images" are biometric data in a recital.

139 SI reservation and AT, DE scrutiny reservation. COM scrutiny reservation.
BE, CZ, DE, DK and SI considered definition too broad. BE queried what "reveal" means. BE also suggested "intending to reveal" in definition (12) and recital (26). In reaction, Cion pointed out that the directive currently in force already uses "reveal". BE: reservation. CZ, SI suggested to insert "specific" before information.

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

141 IT: scrutiny reservation

(13) 'main establishment' means[142]

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes (…) and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented , in this case the establishment having taken such decisions shall be considered as the main establishment[143].

- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

[142] AT remarked that, in view technological developments, it was very difficult to pinpoint the place of processing and , supported by ES, HU, PL, expressed a preference for a formal criterion, which referred to the incorporation of the controller. AT pointed out that such criterion would avoid the situation that, depending on the processing activity concerned, there would be a different main establishment and consequently a different lead DPA.

[143] BE reservation.

(14) 'representative' means any natural or legal person established in the Union who, (…) designated by the controller in writing pursuant to Article 25, represents the controller with regard to the obligations of the controller under this Regulation (…);

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

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings[144];

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

(18) (…)[146]

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

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

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

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

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

145 DE queried whether BCRs could also cover intra-EU data transfers. COM indicated that there was no need for BCRs in the case of intra-EU transfers, but that controllers were free to apply BCRs also in those cases.
HU wanted to include as well non profit organisations.

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

b) data subjects residing in this Member State are substantially[147] affected or likely to be substantially affected by the processing; or

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

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

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

(b) processing which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect[148] data subjects in more than one Member State.

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

an objection as to whether there is an infringement of this Regulation or not, or, as the case may be, whether the envisaged action in relation to the controller or processor is in conformity with the Regulation. The objection shall clearly demonstrate[149] the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects[150] and where applicable, the free flow of personal data.

147 IE and UK would prefer the term 'materially'.
148 Several Member States thought that this should be clarified in recital: CZ, FI, HU, SE.
149 BE thought that this was a threshold too high.
150 IE thought that also risks to the controller should be covered.

(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[151] [152] [153].

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries[154];

[155]

[151] OJ L 204, 21.7.1998, p. 37–48.

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

[153] 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'.

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

[155] **SK proposed new definition: (22) ´public interest´ means an important interest of the Union or Member States pursued in the exercise of public authority which overrides the legitimate interest of the natural person or several natural persons, and without pursuing of which extensive or irreparable damages could arise.**

## CHAPTER II

## PRINCIPLES

*Article 5*

***Principles relating to personal data processing***

1. Personal data must be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject[156];

   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest or *scientific*, statistical[157] or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes[158];

   (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…)[159];

---

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

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

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

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

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

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…); personal data may be stored for longer periods insofar as the data will be processed for archiving purposes in the public interest or *scientific*, statistical, or historical purposes in accordance with Article 83 subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject[160];

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

(f) (…)

2. The controller shall be responsible for compliance with paragraph 1[161].

*Article 6*

***Lawfulness of processing***[162]

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

(a) the data subject has given unambiguous[163]consent to the processing of their personal data for one or more specific purposes[164];

---

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

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

162 DE, AT, PT, SI: scrutiny reservation.
AT submitted suggestions (8408/15)

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

164 RO scrutiny reservation.

(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 of the data subject or of another person;

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

(f) processing is necessary for the purposes of the legitimate interests[165] pursued by the controller or by a third party [166] 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. (…)[167] [168].

2. [169]Processing of personal data which is necessary for archiving purposes in the public interest, or for historical, statistical or scientific purposes shall be lawful subject also to the conditions and safeguards referred to in Article 83.

---

165 FR scrutiny reservation.

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

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

168 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.

169 PL suggested to insert "Without prejudice to processing …."

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

(a) Union law, or

(b) national law of the Member State to which the controller is subject[170].

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.

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

3a. In order to ascertain whether a purpose of further processing (…)[171] is compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent[172], inter alia[173]:

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

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

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

(d) the possible consequences of the intended further processing for data subjects;[174]

(e) the existence of appropriate safeguards[175].

---

171 AT, HU wanted to re-insert "by the same controller".

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

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

174 AT suggested deletion.

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

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected by the same controller, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1[176] [177]. Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject[178] [179].

5. (…)

*Article 7*

***Conditions for consent***

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous[180] consent was given by the data subject.

1a. Where Article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (…) from the other matters, in an intelligible and easily accessible form, using clear and plain language.

---

[176] ES, AT and PL reservation; DE, HU scrutiny reservation. FR suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

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

[178] Cion reservation; AT, BE, BG, DK, ES, FI, HU, IT, LT, PL, SE reservation on paragraph 4 and in particular the last sentence; DE wanted to limit the second sentence to private controllers.

[179] AT, CZ, HU considered the references to the same controller in paragraph (4) inconsistent with paragraph (3a) and proposed to either delete these references or to specify that only the same controller can do further processing
SI: scrutiny reservation.

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

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof[181].

4. (…)

*Article 8*

***Conditions applicable to child's consent in relation to information society services*** [182]

1. Where Article 6 (1)(a) applies[183], in relation to the offering of information society services directly to a child[184], the processing of personal data of a child (…)[185] shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law.

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

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

---

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

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

183 **HU suggested to delete the reference to *information society services directly to a child* or if that is not possible to insert *in particular* after *applies.* HU also wanted to insert a reference to Article 9(2).**

184 Several delegations (DE, HU, ES, FR, SE, SK, PT) disagreed with the restriction of the scope and thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted. **HU suggested to delete "in relation to … child" or to insert "after applies, "in particular".**

185 COM reservation on the deletion of a harmonised age threshold.

3. (…)

4. **(…).**

*Article 9*

***Processing of special categories of personal data***[186]

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

2. Paragraph 1 shall not apply if one of the following applies (…)

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

[186] COM, DK, SE and AT scrutiny reservation. SK thought the inclusion of biometric data should be considered.

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

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

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

(e) the processing relates to personal data which are manifestly made public by the data subject **(…)**; or

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

(g) processing is necessary for (…)[187] reasons of public interest, on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests; or

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

(h) processing[188] is necessary for the purposes of preventive or occupational medicine[189], for the assessment of the working capacity of the employee[190], medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law [191] or pursuant to contract with a health professional[192] and subject to the conditions and safeguards referred to in paragraph 4[193]; or

(ha) (…);

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

(i) processing is necessary for archiving purposes in the public interest or historical, statistical or scientific (…) purposes and subject to the conditions and safeguards laid down in Union or Member State law, including those referred to in Article 83.

---

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

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

190 PL and AT would like to see this deleted.

191 COM, IE, PL scrutiny reservation.

192 FR and PL reservation.

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

(j) (…)[194]

[195]

3. (…)[196]

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

4a. **(…)**[197].

5. Member States may maintain or introduce more specific provisions with regard to genetic data or health data. This includes the possibility for Member States to **(…)** introduce further conditions for the processing of these data[198]**.**

---

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

[195] **SK proposed a new point (k): "processing is necessary for compliance with a legal obligation to which the controller is subject".**

[196] COM reservation on the deletion of paragraph 3 on delegated acts.

[197] Deleted further to the request from COM, CZ, DK, GR, IE, MT, SE, FI and UK scrutiny reservation. FR wanted to keep paragraph 4a in Article 9 or at least keep the text in a recital.

[198] COM scrutiny reservation.

***Article 9a***

***Processing of data relating to criminal convictions and offences***[199]

*Processing of data relating to criminal convictions and offences or related security measures* based on Article 6(1) *may only be carried out either under the control of official authority (…) or when the processing is* (…) *authorised by Union law or Member State law providing for adequate safeguards* for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority[200].

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

[200] SI, SK reservation on last sentence.

*Article 10*

***Processing not requiring identification***

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain or acquire (…) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (…) this Regulation[201].**(…)**

2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification[202].

---

**201** AT, DE, HU, PL scrutiny reservation and UK and FR and COM reservation.

**202** DK, RO, SE and SI scrutiny reservation; COM and FR reservation; FR wanted to add in the end of the paragraph "In any case, the data subject should only have to provide the minimum additional information necessary in order to be able to exercise his or her rights which can never be denied by the controller.

## CHAPTER III

## RIGHTS OF THE DATA SUBJECT[203]

### SECTION 1

### TRANSPARENCY AND MODALITIES

*Article 11*

***Transparent information and communication***

1. (…)

2. (…)

**203** General scrutiny reservation by UK on the articles in this Chapter.

*Article 12*

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

1. The controller shall take appropriate measures[204] to provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language[205]. The information shall be provided in writing, or by other [206]means**,** where appropriate electronically[207]. Where the data subject makes the request in electronic form, the information may as a rule be provided in electronic form, unless otherwise requested by the data subject. When requested by the data subject, the information may[208] be given orally provided that the identity of the data subject is proven.[209] [210] [211] [212]

---

[204] AT, supported by MT, PL, suggested to delete the text *take appropriate measures,* in contrast DE wanted to keep this phrase.

[205] AT suggested adding: "and adapted to the data subject".

[206] SI suggested to insert "demonstrable".

[207] SE did not see any added value in *or where appropriate, electronically,* in contrast to CZ and PL, which wanted to keep this phrase.
AT meant that the information could be provided orally as long as the data subject agreed to that. COM found that idea sympathetic.
AT made a suggestion for the second sentence of paragraph 1 (7586/15 REV1)
IE was not convinced that data subjects under all circumstances could receive information in paper form.

[208] SK, suggested "must" instead of "may".

[209] UK suggested that the paragraph could also refer to machine readable information.

[210] IE opposed obliging the data controller to provide personal data in paper form in all cases as this could be burdensome and costly.

[211] DE suggested to add at the end "if this does not involve a disproportionate effort".

[212] DK, supported by FI, suggested to delete the last two sentences of the paragraph considering these too detailed and, because they do not take into account that electronic information sometimes cannot be provided for instance for security reasons or because the controller does not have that information in electronic form. In reaction, Cion, supported by DE and FI, suggested "may as a rule".
DE suggested to insert at the end "if this does not involve a disproportionate effort".

1a. [213]The controller shall facilitate[214] the exercise of data subject rights under Articles 15 to 19[215]. (…) In cases referred to in Article 10 (2) the controller shall not refuse to act on the request of the data subject for exercising his/her rights under Articles 15 to 19, unless the controller demonstrates that.[216] he is not in a position to identify the data subject.

2. The controller shall provide **(…)** information on action taken on a request under Articles 15 and 16 to 19 to the data subject without undue delay and at the latest within one month[217] of receipt of the request (…). 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.

---

213 CZ, DK, IE, FI, FR, SK, UK: reservation.
PL scrutiny reservation on relation between the last sentence of paragraph 1a and Article 10(2).
AT scrutiny reservation. AT pointed to the relation with Article 12(4a).
BE, supported by EE, FR, pointed to the importance of making the digital identification, for example through a log-in or an e-mail address, besides the identification of a physical person.

214 CZ suggested instead: "The controller shall not make any obstacles to…"

215 SI, CZ and UK thought this paragraph should be deleted because already covered by Article 10(2).

216 UK suggested to delete "demonstrates that he" to align with Article 10(2).

217 FR suggested a two months' period. UK said that the 1995 Directive uses '*without excessive delay'* and suggested to use it here too. FR and UK wanted to extend the deadline. CZ, SI, 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. SI suggested to say 'in accordance with law' because the MS have general rules on deadlines. SK wanted a fixed deadline with flexibility of one month. ES and Cion said that a deadline was necessary, ES supporting a one month deadline.

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

4. Information provided under Articles 14 and 14a (…)[218] and any communication under Articles 16 to 19 and 32 shall be provided free of charge[219]. Where requests from a data subject are *manifestly* unfounded[220] or excessive[221], in particular because of their repetitive character[222], 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.

4a. [223]Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity[224] 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. (…)

---

218 UK wanted to see the reinsertion of a reference to Article 15.

219 SE thought that since information in Article14 was to be provided by the data subject it did not fit in the context to talk about free of charge.

220 DE, supported by BE, ES and PL suggested to say *abusive* instead of manifestly unfounded. Also DE preferred "abusive". SI thought that *abusive* could be used in a recital. IE, AT, DK, UK, PT, NO, RO, HR, EL, SI, CY, FI, CZ, LT, SE,SK, MT supported the term “manifestly unfounded”.

221 PL, supported by SE, thought that the criterion of 'manifestly excessive' required further clarification, *e.g.* through an additional recital.
CZ found the wording complex and suggested to grant the data subject the right to request information every 6 months.

222 AT suggested to delete "in particular of their repetitive character".

223 AT suggested a recital on identification of the data subject (7586/15 REV1)

224 SI suggested to replace *identity* with *authentification.*

*Article 13*

***Rights in relation to recipients***[225]

*(…)*

**SECTION 2**

**INFORMATION AND ACCESS TO DATA**

*Article 14*

***Information to be provided where the data are collected from the data subject***[226]

1. Where personal data relating to a data subject are collected from the data subject, the controller shall (…),at the time [227]when personal data are obtained, provide the data subject with the following information:

---

225 FR suggested a new Article 13a on standardised information policies, or, alternatively a recital, with the following wording: 'In order to ensure that the information to be provided to the data subjects according to this Regulation will be presented in an easily visible and clearly legible way and will appear in a language easily understood by the data subjects concerned, the European Data Protection Board shall issue guidelines to further specify the requirements for specific categories of processing or specific data processing sectors, including by issuing aligned tabular, using text and symbols or pictographs.' that is inspired by a suggestion by the EP.

226 DE, 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. DE found the EP idea of providing information in the form of symbols was an interesting idea which facilitates the provision of information. SE found it peculiar that for example a court would be obliged to provide separate information to the data subject about a case that the data subject had initiated; such obligations are set out in the code on procedure.

227 UK, supported by CZ, suggested to have instead: "as soon as / where practicable,". In reaction, Cion indicated that this would lower the level of data protection compared to the Directive 95/46/EC.
DE suggested to insert "where appropriate". In response, Cion indicated that "where appropriate" is not possible because the moment that the controller would ask data from the data subject it must inform the data subject.

(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall 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 (…) as well as the legal basis of the processing[228].

1a. [229]In addition to the information referred to in paragraph 1, the controller shall[230] at the time when personal data are obtained [231]provide the data subject with such further information[232] that is necessary to ensure fair and transparent processing (…) [233], having regard to the specific circumstances and context in which the personal data are processed[234]:[235]

---

228 Suggestion of AT, HU, PL, SK. Opposed by DK, SE.

229 UK found the list too long considering that more discretion is needed so that information should be provided when it would have added value.

230 DE, and PL asked to insert "on request". DE, DK, NL and UK doubted whether the redraft would allow for a sufficient risk-based approach and warned against excessive administrative burdens/compliance costs. NL, supported by CY and CZ, suggested therefore to add 'where appropriate' after *shall.* DK and UK in particular referred to the difficulty for controllers in assessing what is required under para. 1a in order to ensure fair and transparent processing. DE and PL pleaded for making the obligation to provide this information contingent upon a request thereto as the controller might otherwise take a risk-averse approach and provide all the information under Article 14(1a), also in cases where not required. UK thought that many of the aspects set out in paragraph 1a of Article 14 (and paragraph 2 of Article 14a) could be left to guidance under Article 39. DE, supported by IT, suggested to insert 'at the time when the personal data was obtained'. In contrast, IT thought that it was not necessary to provide the information at the same time.

231 DE suggestion supported by Cion and PL.

232 CZ suggested adding the word 'obviously'.

233 Deleted at the suggestion of FR. AT, opposed by Cion, wanted to delete the end of the sentence from 'having regard …'

234 COM reservation, supported by ES, on deletion of the words 'such as'. AT preferred the COM proposal because in particular the new paragraph 1a was drafted in a too open and vague manner, therefore the NL suggestion to add *where appropriate* went in the wrong direction. IT was against reducing the safeguards and considered the text as the bare minimum.

235 CZ, supported by Cion, suggested to insert again the reference to the data subject.

(a) (…);[236]

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

(c) the recipients or categories of recipients of the personal data[237];

(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 (…) as well as the right to data portability [238];

(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2)[239], the existence of the right to withdraw consent[240] at any time[241], without affecting the lawfulness of processing based on consent before its withdrawal;

(f) the right to lodge a complaint to a supervisory authority (…)[242];

---

236 BE, supported by FR, HU, IT, MT, SK, PL, wanted either to reintroduce the text of Article 14(1)(c) on storage period or add as the EP has done *the criteria used to determine the period.* Cion also supported the reinsertion on text on a storage period.

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

238 BE suggestion, supported by COM. The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE. IT said that the information in paragraphs (e) and (f) were set out in Article 8 of the Charter and always had to be provided and therefore needed to be included in paragraph 1.

239 DE suggested to delete "or point (a) of Article 9(2)".

240 DE suggested to insert "pursuant to Article 7(4).

241 DE suggested to insert a reference to Article 7(3).

242 IT said that the information in paragraphs (e) and (f) were set out in Article 8 of the Charter and always had to be provided and therefore needed to be included in paragraph 1.AT supported this concerning point (e) (7586/2/15).

(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 whether the data subject is obliged to provide the data and of the possible consequences of failure to provide such data[243];

*(h)* [244]*the existence of* automated decision making including *profiling referred to in Article 20(1) and (3) and information concerning* (…) the logic involved [245]*, as well as the significance and the envisaged consequences of such processing for the data subject.* [246]

---

243 CZ, DE, ES reservation.

244 PL suggested: "where applicable, information about the existence of profiling referred to in Article 4(12a) and/or about automated decision making referred to in Article 20(1) and (3) and information concerning….".

245 SE preferred to delete the phrase "the logic involved".
AT pointed out need to make terms consistent in this paragraph and Articles 14a(2) and Article 15(1)(h).

246 SE scrutiny reservation. IT meant that there were problems with this paragraph if the current text of Article 20 was maintained. DK suggested to delete this point considering it too burdensome.

1b. Where the controller intends to further[247] process the data **(...)** for a purpose other than the one for which the data were collected the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 1a.[248] [249]

2. (…)[250]

3. (…)

4. (…)

[247] DK, IE, FR reservation.
DE: scrutiny reservation.

[248] UK suggested to delete this paragraph.
AT meant that the paragraph was relevant and important. FR, IT, PL, RO, NO and COM supported paragraph (1b).

[249] BE, PL pointed out that Article 14(1b) and Article 14a(3a) should use consistent wording. DE made a suggestion (8089/15/).
Cion opposed the DE suggestion referring to Article 21 which allows Member States to restrict of the obligations and rights in inter alia Article 14 and 14a. Moreover, Directive 95/46/EC does not provide for such restrictions and therefore the DE suggestions would lower the level of data protection.
DK considered the wording of the paragraph less clear now that the reference to Article 6(4) has been deleted and wanted to await the outcome of the horizontal discussion on further processing. DE, supported by FR, pointed out that it understood the paragraph to concern both compatible and incompatible purposes given that that the reference to Article 6(4) which refers to incompatible purposes only was deleted.

[250] HU and AT reservation on the deletion of this paragraph.
DE made a suggestion (8089/15)

5. Paragraphs 1, 1a and 1b[251] shall not apply where and insofar as the data subject already has the information[252],

[253]

6. (…)

7. (…)

8. (…)

*Article 14 a*

***Information to be provided where the data have not been obtained from the data subject[254]***

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information[255] [256]:

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

---

[251] Suggestion by CZ, DK, NL, SE and NO.
ES considered that the reference to paragraph 1b could be deleted.

[252] SE, supported by CZ, thought that it was necessary to insert more exceptions to the obligation to provide information SE mentioned such as illness or a fire. COM cautioned against limiting Article 14 too much. SE further considered that a similar provision to the one in Article 14a(4)(c) should be added. SE noted that recital 50 did not make a difference between the situations in Article 14 and 14a. Article 21 on restrictions would be difficult to use to create exceptions considered SE.
PL made a suggestion (8295/15).

[253] DE, on the substance supported by MT, suggested to add a new point (f): "where the data are processed by a micro enterprise which processes data only as an ancillary activity.

[254] DE, ES, AT, PT scrutiny reservation.

[255] DE suggested to add: "where appropriate".

[256] RO wanted tot add that this information should be provided once per year.

(b) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing[257].

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information that is necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context[258] in which the personal data are processed (…)[259]:

(a) the categories of personal data concerned;

(b) (…)[260]

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

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

(da) 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[261] concerning the data subject and to object to the processing of such personal data as well as the right to data portability (…);

---

257 Suggestion of HU, AT, PL and SK. Opposed by DK, SE.
PL also suggested a new point: "the origin of the personal data, unless the data originate from publicly accessible sources".

258 IT and FR doubts on the addition of the words 'and context'.

259 DE suggested to add: "at the time when personal data are processed for the first time".

260 BE, IT, FR, HU, MT, SK, PL, supported by Cion, wanted, as in Article 14(1a), a text on storage period or add as the EP has done *the criteria used to determine the period.*

261 Suggestion of SE.

(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

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

(g) [262]from which source the personal data originate, unless the data originate from publicly accessible sources[263]; [264]

*(h) the existence of* automated decision making including *profiling referred to in Article 20(1) and (3) and*[265] *information concerning* the logic involved[266]*, as well as the significance and the envisaged consequences of such processing for the data subject.*[267]

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

(a) within a reasonable period after obtaining the data, but at the latest within one month[268], 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.

---

262 Suggestion of DE. PL suggested to move this point to paragraph 1.

263 Cion and AT scrutiny reservation. BE, supported by ES and SE, suggested to delete paragraph (g). AT (7586/2/15), IT suggested to delete the phrase: "unless…. sources".

264 Cion reservation (in line with position on the deletion of paragraph 4(d). PL suggested to move point (g) to paragraph 1.

265 PL suggested instead "and/or".

266 SE considered the phrase "the logic …processing" unnecessary because already covered by Article 15(1)(h).
AT pointed out the need to make terms consistent between this paragraph and Articles 14a(2) and Article 15(1)(h).

267 DK suggested to delete this point considering it too burdensome.

268 CZ reservation on one month fixed period.

3a Where the controller intends to further [269]process the data (…) for a purpose other than the one for which the data were obtained[270], the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.[271][272]

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

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

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort [273] [274]; in such cases the controller shall take appropriate measures to protect the *data subject's* rights and freedoms and legitimate interests[275]; or

---

269 DK, FR, IE: reservation
DE: scrutiny reservation.
DE, FI, PL queried what "purpose other than the one for which the data were obtained" meant.

270 CZ scrutiny reservation on concept of obtaining data.

271 IT meant that paragraph 3a represented the bare minimum of protection. AT support of the paragraph. UK meant that it should be used taking into account proportionality and practicability.
DK, FI considered the wording of the paragraph less clear now that the reference to Article 6(4) has been deleted. DK would await the outcome of the horizontal discussion on further processing.

272 DE made a text suggestion (8089/15).

273 FR and AT asked what the words *or is likely … purposes of the processing* were supposed to mean. COM wanted to delete that part of the paragraph. CZ wanted to keep the text in order to avoid fraud. COM noted that it was important to avoid fraud but considered that Article 21 gave the necessary flexibility for that.

274 Suggestion of ES, FR, supported by Cion, to delete the phrase " or is likely to render impossible or to seriously impair the achievement of the purposes of the processing". CZ, DE opposed deletion of this phrase.
COM scrutiny reservation.

275 Several delegations (FI, PL, SI, 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.

(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[276]; or

(d) (...)[277];

(e) where the data must remain confidential in accordance with Union or Member State law **(...)**[278].[279]-[280]

**281**

5. (…)

6. (…)

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

**277** The phrase "where the data originate from publicly accessible resources, or" was deleted at the request of a large number of delegations. CZ, DE, SE and UK emphasised the importance of this exception given the quantity of data published on the internet. In reaction Cion indicated that re-instating this phrase would bring the risk of profiling without the subject knowing.

**278** COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality).

**279** IT said that the information in paragraphs (e) and (f) were set out in Article 8 of the Charter and always had to be provided and therefore needed to be included in paragraph 1.

**280** CZ proposed to re-insert the text "or because of the overriding legitimate interests of another person".

**281** DE**,** on the substance supported by MT, suggested to add a new point (f): "where the data are processed by a micro enterprise which processes data only as an ancillary activity.

*Article 15*

***Right of access for the data subject***[282]

1. The data subject shall have the right to obtain from the controller[283] [284]at reasonable intervals and free of charge[285] (…) confirmation as to whether or not personal data concerning[286] him or her are being processed [287]and where such personal data are being processed access to the data and the following information:

   (a) the purposes of the processing[288];

   (b) (…)

   (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries[289] or international organisations[290];

   (d) where possible, the envisaged[291] period for which the personal data will be stored;

---

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

283 FR suggested to add a right of access to processors.

284 DE suggested to insert "on request".

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

286 FR suggested to change *concerning* to *belonging* so that different forms of telecommunication would be covered. COM said that *concerning* was used in Article 8 in the Charter.

287 DE made a text suggestion (8089/15).

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

289 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.

290 Presidency suggestion to be consistent with paragraph (1a), Article 14a(d) and 14a(2)(da).

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

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of the processing 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 (…)[292] [293];

(g) where the personal data are not collected from the data subject, any available information as to their source[294];

(h) [295]in the case of decisions based on automated processing including profiling referred to in Article 20(1) and (3), information concerning the logic involved[296] as well as the significance and envisaged consequences of such processing[297].

1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer[298].

---

292 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.

293 IT and SK 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.

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

295 PL made a suggestion (8295/15).

296 PL reservation on the reference to 'logic': the underlying algorithm should not be disclosed. SE wanted to delete it. BE and IT opposed the deletion of the words *logic* because it would go below the level of the 1995 Directive (Article 12(a)). DE reservation on reference to decisions.

297 FR harboured doubts on its exact scope.
DE suggested to redraft point (h): " Redraft point (h) as follows: "in case of decisions based on automated processing including profiling referred to in Article 20(1) and (3), ~~knowledge of and~~ information concerning the logic involved ~~in any automated data processing~~ as well as the significance and envisaged consequences of such processing; the right to obtain this information shall not apply in particular where trade secrets of the controller would be disclosed."

298 FR and UK scrutiny reservation on links with Chapter V.

1b. On request [299]and without an excessive charge[300], the controller shall provide a copy of the personal data undergoing processing to the data subject.

2. **(…)**

2a. [301]The right to obtain a copy referred to in paragraph 1b **(…)** shall not apply where such copy cannot be provided without disclosing personal data of other data subjects or confidential data of the controller. Furthermore, this right shall not apply if disclosing personal data would infringe intellectual property rights in relation to processing of those personal data.[302] [303] [304] [305] [306].

3. (…)

4. (…)

---

[299] FR made a suggestion for paragraph (1b) in 7464/15.

[300] ES wanted no charge except in case that the costs are very high or that the data subject requests a special format.

[301] AT, ES: scrutiny reservation.
PT suggested to clarify in a recital that access to intellectual property rights can be obtained in return for a payment.
DE made a text suggestion (8089/15).

[302] UK suggestion

[303] Cion reservation considering that the paragraph restricts too much the right to obtain a copy of the personal data and referred to the possibility to restrict this right if the requirements of Article 21(1)(f) are met..
DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.

[304] FR suggested to add "which were not supplied by the data subject to the controller".

[305] DE suggested to add a new paragraph (2a): "There shall be no right of access in accordance with para-graphs 1 and 1b when data are processed by, or are entrusted to become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statuary obligation of secrecy, except if the data subject is empowered to lift the secrecy in question and acts accordingly."

[306] DE suggested a new provision: "There shall be no right of access in accordance with paragraphs 1 and 1b when data are processed by, or are entrusted to become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation, except where the subject is empowered to lift the secrecy in question and acts accordingly."

## SECTION 3

## RECTIFICATION AND ERASURE

*Article 16*

***Right to rectification***[307]

1. (…) The data subject shall have the right[308] to obtain from the controller without undue delay[309] 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. (…)

---

307 DE and UK scrutiny reservation.

308 UK, supported by CZ, suggested to insert the qualification ' where reasonably practicable'

309 UK, supported by CZ, also suggested inserting the qualification 'where necessary'. Suggestion from the SE.

*Article 17*

***Right to erasure and "to be forgotten"***[310]

1. [311]The (…) controller shall have the obligation to erase personal data without undue delay,

[310] SI reservation on "right to be forgotten".
FR, RO, 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, 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 (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, SI and UK).
It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LU, SE and SI).
AT made a suggestion to distinguish the right to erasure and the right to be forgotten (7586/15 REV1).

[311] SE suggested to insert in the beginning of the sentence *At the request of the data subject, the controller* …to indicate that the controller was not supposed to act at its own initiative.

especially in relation to personal data which are collected when the data subject was a child, and the data subject[312] shall have the right to obtain from the controller [313] the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

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

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) and (…) there is no other legal ground for the processing of the data; [314]

(c) the data subject objects to the processing of personal data[315] *pursuant to Article 19(1)* and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2);

[312] SE wanted to delete the part of the text from *without* until *and the data subject.*
[313] Suggestion of DE, supported by Cion.
[314] AT asked if this referred to further processing and wanted that to be clarified in a recital.
[315] NL suggested to refer to a specific request for erasure pursuant to Article 19(1).

(d) the data have been unlawfully processed[316];

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[317];

1a The data subject shall have also the right to obtain from the controller the erasure of personal data concerning him or her, without undue delay, if the data have been collected in relation to the offering of information society services referred to in Article 8(1).[318]

(…).

2. (…).

316 UK and CZ scrutiny reservation: this was overly broad.

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

318 PL: reservation considering the reference to children in the introductory part sufficient. HU reservation considering the restriction to information society services too narrow.

2a. *Where the controller[319] (…) has made the personal data public[320] and is obliged pursuant to paragraph 1 to erase the data,* the controller, taking account of available technology and the cost of implementation[321], *shall*[322] take (…) reasonable steps[323], including technical measures, (…) to inform controllers[324] which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data[325].

---

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

320 DE suggested to add "or has transmitted them to a recipient".
ES preferred 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.

321 Further to NL suggestion. This may hopefully also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology. FR raised doubts about the fact that the provision was only applicable when the data had been made public.

322 CZ, FI, IE, NL, PL, UK, wanted to reinsert "at the request of the data subject" in Artcile 17(3) and the corresponding recital (54) arguing that the data subject would not know that there is data concerning him. NL wondered how the controller could know without a request of the data subject that certain information would need to be erased.
AT, CY, HU, FR, MT, supported by Cion, could accept not having this phrase.

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

324 PL, UK wanted to keep "known" controller. UK argued that in order to compare the standards of Directive 95/46/EC with those of the new regulation need to be considered in light of the explosive growth of Internet. Moreover, UK pointed out that the directive refers to disproportionate efforts whereas paragraph 2a of the regulation does not have such a reference; against that background, UK would consider the limitation to "known" controllers justified.
PL made two alternative suggestions (8295/15).
SK suggested to refer instead to controllers with whom the controller has contractual relations.

325 FR suggested to add "and on which grounds that request was accepted". BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule. ES and PL suggested to delete paragraph 2a. HU found the content of paragraph (2a) not clear as it refers at the same time to an obligation to erase data and to cases where the data subject requested erasure. As a result, it is unclear whether the paragraph applies or not in cases of erasure not on request of the data subject but on other grounds.

3. Paragraphs 1**,** 1a and 2a shall not apply[326] to the extent that (…) processing of the personal data is necessary:

a. for exercising the right of freedom of expression and information[327] [328];

*b.* *for compliance with a legal obligation* which requires *processing* of *personal data by Union or Member State law to which the controller is subject*[329][330] or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[331];

---

[326] 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.

[327] FR queried whether the right to information should be included in the Article considering that this right is linked to Article 80 which does not include search engines. In reaction, Pres argued that the provisions on data controllers apply to search engines. Furthermore, Cion indicated that the freedom of expression and information is in the Charter and therefore the reference in Article 17(3)(a) will not change the interpretation of Article 80.

[328] FR suggestion to delete "referred to in Article 80". This would than cover the other FR suggestion, which was supported by CY, IE, IT, to insert a new point (aa): "for the interest of the general public to have access to that information". Cion considered that the phrase "referred to in Article 80" has added value as it indicates that it is up for the Member States to reconcile in their national law the right to the protection of personal data with freedom of expression and information.
DE and EE asked why this exception had not been extended to individuals using their own freedom of expression (e.g. an individual blogger).

[329] FI suggestion, supported by DE and COM, to narrow down the scope.

[330] 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, supported by IE, 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).

[331] AT, PL scrutiny reservation. PL suggested: to add "when expressly laid down by Union or Member States law".

c. for reasons of public interest in the area of public health in accordance with Article 9(2) (h)[332] and (hb) as well as Article 9(4)[333];

d. [334]for archiving purposes in the public interest or for *scientific, statistical* and historical (…) purposes in accordance with Article 83[335];

e. (…)

f. (…)

g. for the establishment, exercise or defence of legal claims.[336]

4. (…)

5. (…)

[332] COM thought that (h) should be deleted.

[333] 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.

[334] FR considered point (d) not needed because of Article 83. Previously, FR has suggested to move "in the public interests" after "purposes" in order to extend the limitation provided for archiving purposes to the other purposes.
AT considered a global provision inadequate for applying data protection rules in specific cases.

[335] DE suggested: ".. and historical purposes where the erasure would involve disproportionate effort or processing is essential for those purposes ~~in accordance with Article 83~~" .Cion opposed this suggestion considering that it would do away with the obligation in Article 83 to provide safeguards.

[336] DE suggested a new paragraph 3a "Where the erasure is carried out, the controller shall not otherwise process such data".

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)[337] the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[338];

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

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

2. (…)

3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest[339].

---

337 FR considered the wording of point (a) ambiguous.

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

339 DE and SI asked who was to define the concept of public interest. DE reservation.

4. A data subject who obtained the restriction of processing pursuant to paragraph 1 (…) shall be informed by the controller before the restriction of processing is lifted[340].

5. (…)

5a. (…)[341]

[340] DE, PT, SI and IT thought that this paragraph should be a general obligation regarding processing, not limited to the exercise of the right to be forgotten. DK likewise thought the first sentence should be moved to Article 22. FR preferred the previous version of the text.

[341] Deleted in view of the new article 83.

*Article 17b*

***Notification obligation regarding rectification, erasure or restriction***[342] [343]

The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each[344] recipient to whom the data have been disclosed **(…) ,** unless this proves impossible or involves disproportionate effort.

[342] 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) 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, supported by PL, was opposed to a general obligation to log all the disclosures to recipients. DE, supported by PL, 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.

[343] DE suggested a new Article 17c on dispute settlement (7567/15). Supported by IE, FR and opposed by IT.

[344] DE suggested: "The controller shall inform the data subject about those recipients if the data subject requests this."

*Article 18*

***Right to data portability***[345]

1. (…)

[345] 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 (DE, FR, 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.
SI: scrutiny reservation.
CZ thought its scope should be limited to social media.
DE and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to/raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, FI, HU, SE and UK also underscored the considerable administrative burdens this article would imply. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger on-going research or the continuity of the service. Reference was also made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK).
DE, ES, FR, HR, PL and NO were in principle supportive of this right. SK thought that the article was unenforceable and DE, supported by HU, 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, for example group photos. HU therefore questioned the added value of this right.
CZ, DE, DK, FI, RO and NO thought that the exclusion of the public sector should be mentioned not only in recital 55, but also here (ES was opposed thereto).
ES, FI, FR,MT (7464/15) and RO, supported by Cion, wanted data portability to mean the transmission of data from one controller to another. However, a majority of delegations see the right to portability as the right to get at copy without hindrance and to transmit that data to another controller.
FI did not want an obligation for the systems of the controllers between whom data are transmitted to be interoperable. In response, Cion indicated that such obligation would not be created as it only concerns a right for a data subject to withdraw.

2. The data subject shall have the right to receive[346] the personal data[347] concerning him or her[348], which he or she has provided to a controller[349], in a structured and[350] commonly used[351] and[352] machine-readable format and have the right to transmit those data to another controller[353] without hindrance from the controller to which the data have been provided, where

(a) the processing is based on consent pursuant to point (a) of Article 6(1)or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and

(b) the processing is carried out by automated means[354].

---

346 FI, IT preferred the term *withdraw.* EL, HU, supported by Cion preferred *obtain.*
UK reservation on "withdraw" considering that "withdraw" has the connotation of leaving no data behind and, therefore, duplicates the right to erasure. UK suggested instead "obtain (a copy for further use)". FR did not agree with the UK views considering it possible to use the right to erasure and data portability in parallel.

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

348 DE, FR wanted to re-insert in Article 18(2) and in recital (55) the phrase "and any other information" considering that not having this phrase would decrease the scope of data portability too much.
**Cion scrutiny reservation.**
CZ, DK, HR, SE supported not taking up "and any other related information.

349 AT suggested instead the term "service provider" making also a suggestion for modification (8089/15).

350 Consistency of language with Article 15(2).

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

352 PT thought 'and' should be deleted.

353 CZ suggested to delete "and have the right to transmit those data to another controller.

354 DE, ES and FR thought emphasis should be put on the right to withdraw data, also with a view to creating an added value as compared to the right to obtain a copy of personal data. CY and HU also thought the obligation of the controller should be emphasised.

2a. The exercise of this right shall be without prejudice to Article 17. The right referred to in paragraph 2 shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [355][356]

2aa. The right referred to in paragraph 2 shall not apply if disclosing personal data would infringe intellectual property rights in relation to the processing of those personal data[357].

3. (…)[358]

4. (…)[359].

[355] IT: scrutiny reservation on last sentence.
CY, EL and Cion suggested instead: "The right referred to in paragraph 2 shall not apply to processing carried out by public authorities or bodies".

[356] FR preferred wording related to the public purpose rather than to the public bodies.

[357] Cion reservation
ES thought there should be an exception in case disproportionate efforts would be required.

[358] PL reservation on deletion
BE thought that standard contractual clauses should always remain facultative.

[359] Deleted in view of the new Article 83.

## SECTION 4

## RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION MAKING~~PROFILING~~

*Article 19*

***Right to object***[360]

1. [361]The data subject shall have the right to object, on[362] grounds relating to his or her particular situation[363], at any time to the processing of personal data concerning him or her which is based on points (…) (e) or (f) of Article 6(1), **the first sentence of Article 6(4) in conjunction with point (e) of Article 6(1) or the second sentence of Article 6(4)**[364].

---

[360] AT made a suggestion for modification (8089/15).
FR made suggestions to modify Article 19 (7464/15). Furthermore, FR wanted data subjects to have the right to object in case of processing for purposes covered by Article 9(2)(i) unless this processing is done for public interest purposes.
PL did not want a right to object in relation to processing referred to in Article 83.

[361] FI, IE, UK suggested to use the wording of Article 14 of the directive currently in force.

[362] CZ, DE, FI, IE, UK reservation on deletion of "compelling legitimate" in Article 19(1). However, these delegations could accept re-insertion of (e) provided re-insertion of "compelling legitimate". CZ suggested: "1. The data subject shall have the right to object, at any time: (a) on compelling legitimate grounds to the processing of personal data concerning him or her which is based on point (e) of Article 6(1), (b) on grounds relating to his or her particular situation to the processing of personal data concerning him or her which is based on point (f) of Article 6(1).
AT, DK, FR, MT, PL rejected having "compelling legitimate" in the first line of the proposal in document 7978/1/15 REV1.Cion considered" compelling legitimate" not acceptable given Article 6(1)(f) and because it undermines making use of the right to object. This wording would allow that even compelling legitimate grounds of the data subject could be overridden by the controller; this would go below the protection level of Directive 96/46.
The reference to point (e) of Article 6(1) was restored in view of the support of PL, IT, DK, ES, DE, RO, SI, AT, EL, CY. Including (e) was objected by UK, DE, BE, CZ, FI, HU and NL.
COM stated that 1995 Directive contained a reference to point (e). 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. ES asked that a reference to Article 6(2) be added.

[363] AT suggested to delete "relating to his or her particular situation" because the right to object is a fundamental human right.

[364] **New Presidency suggestion**
**AT, HU, IT, LT expressed that a reference to Article 6(4) was not sufficient to take away their reservation on Article 6(4) as such.**
**HU suggested to make also a reference to Article 9(2).**

The controller shall *no longer process* the personal data (…) unless the controller demonstrates compelling legitimate grounds[365] for the processing which override the interests, (…) rights and freedoms of the data subject[366] or for *the establishment, exercise or defence of legal claims*. [367][368]

[365] DE: scrutiny reservation.
IE suggested instead reasoned legal grounds" or using the text of the directive currently in force.

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

[367] Moved from paragraph (1a). 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, 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.

[368] FR suggested to insert a new paragraph 1ab in order to allow data subjects to object to the further processing of his/her data based on Article 6(4). "Where the controller intends to further process the data on the basis of Article 6, paragraph 4 for other purposes than the one for which the data were collected, the possibility of the right to object shall be brought explicitly to the attention of the data subject and where an objection is upheld, the personal data shall no longer be processed."

1a. **(…)**

2. Where personal data are processed for direct marketing[369] purposes, the data subject shall have the right to object[370] (…) at any time to the processing of personal data concerning him or her for such marketing. At the latest at the time of the first communication with the data subject[371], this[372] right[373] shall be explicitly brought to the attention of the data subject (…) and shall be presented clearly and separately from any other information[374].

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

---

369 FR and UK underlined 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.

370 DE suggested to insert: "free of charge".

371 IT preferred "prior to processing".

372 Suggestion by BE opposed by IE.
DE, supported by PL and preliminary BE suggested instead: "In approaching the data subject,".

373 DE suggestion, supported by COM, to inform the data subject as soon as possible of the right to object.

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

2aa. Where personal data are processed for historical, statistical or scientific purposes the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest[375] .[376]

[375] Reservation: AT, CZ, ES, LT, PT doubting the need for this paragraph. AT, PT noted that a data subject that finds out that a historical document is fake must have the possibility to object. Furthermore, given that statistics present aggregated data there is less of a protection need. CZ missed specificities about what the public interest is (supported by FI) and who is going to make the assessment. In response, Cion indicated that Article 6(3) specifies the determination what is in the public interest, namely Union or national law.
BE, NL scrutiny reservation. NL noted that processing can also be done in the public interests and for gainful purposes at the same time, for instance development of new pharmaceutical cures.
DE could accept the text of paragraph (2aa) provided that Article 6(2) remained unchanged.
FI positive provided that Article 6 and 9 remain unchanged.
SE suggested to replace "performance of a task carried out for reasons of public interest" with "fulfilment of these specific purposes".
FR, HR, UK considered the references to public interest at the beginning and the end of the paragraph to be inconsistent.
FR proposal to insert a new paragraph: 2b „Where personal data are processed for historical, statistical or scientific purposes on the basis of point (i) of Article 9(2), the data subject shall have the right to object at any time to the processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. Prior to the processing, this right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information and where an objection is upheld, the personal data shall no longer be processed.

[376] **IE wanted to keep at the end of the paragraph the phrase: "or for compliance with a legal obligation to which the controller is subject". AT wanted to delete the paragraph and SE had serious concerns.**
FR, SI, requested clarification what was meant by a legal obligation: a basis in Union or national law or also for example a contract?

3. (...)

4. (…)

*Article 20*

***Automated individual decision making***[377]

1. The data subject shall have the right not to be subject to a decision **(…)**[378] based solely[379] on automated processing, including profiling[380], which *produces legal effects* concerning him or her or [381]significantly [382] affects him or her.[383]

---

377 DE, ES, FR, AT, HU, PL, SE and UK scrutiny reservation.
DE found further changes needed to avoid that the Article would result in discrimination.
AT suggested: "Decision making based on automated personal processing".
IT, supported by PT, reservation considering the concept of profiling laid down in the Presidency text too narrow. IT wanted to re-insert a definition of "profile" and to modify the definition of "profiling" in line with the ideas of the Council of Europe report of 2010.
AT suggested to dispense with the concepts of profiling and profile in the text.
DE made a suggestion to add paragraphs to Article 20 (8089/15).
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).
ES was not favourable to the new drafting and asked that the objective was. DE stressed that it was important to look at the definition of profiling in order to ensure consistency. IT said that the way the Article was drafted it dealt with decisions based on profiling and not profiling as a technique. IT noted that for example fingerprints and exchanges between machines would be more common in the future.

378 ES wanted to delete the words from *a decision* until *him or her.*

379 PL suggested "predominantly" instead of "solely".

380 AT suggested to delete profiling and replace it with "such" (8089/15).
Scrutiny reservation: SI.

381 CZ suggested to insert "similarly". In reaction, Cion indicated this would lower data protection standards.

382 PL suggested to clarify in a recital the meaning of "significantly affects him or her".
DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there are also cases of automated data processing which actually were aimed at increasing the level of data protection (e.g. in case of children that are automatically excluded from certain advertising). IT was concerned about the word *significantly* and wanted it clarified in a recital. COM meant that it could be clarified in a recital.

383 DE meant that the title and definition in Article 4(12a) required a particular need for clarification.

1a. Paragraph 1 shall not apply if the decision[384]: (...)

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller **(…)**; 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 rights and freedoms and legitimate interests; or

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

1b. In cases referred to in paragraph 1a (a) and (c)[385] the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least[386] the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision:

2. (…)

---

[384] COM suggestion.

[385] IE suggestion.
PL suggested instead to refer to "Article (1a)".

[386] BE suggestion, supported by FR.

3. [387]Decisions referred to in paragraph 1a shall not (…) be based on special categories of personal data referred to in Article 9(1), unless points (a) or (g)[388] of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests [389] are in place.

4. (…)

5. (…)[390]

[387] SK considered the paragraph to provide insufficient guarantees.

[388] UK did not want to limit processing to only points (a) or (g) so it suggested to delete the reference to points (a) and (g) whereas HU wanted to add point (c).

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

[390] DE suggested new paragraphs 4-6 (7586/15) because of particular constitutional sensitivities.

## SECTION 5
## RESTRICTIONS

*Article 21*

***Restrictions***[391]

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in (…) Articles 12 to 20 and Article 32, as well as Article 5[392] in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

   (aa) national security;

   (ab) defence;

   (a) public security;

   (b) the prevention, investigation, detection ~~and~~ **or** prosecution of criminal offences[393] or the execution of criminal penalties **or the safeguarding against and the prevention of threats to public security**;

---

391 DE suggested a new recital (48a) (7586/1/15 REV1).
AT recalled the note of AT, SI, HU to the 3354th Council.
SI and UK scrutiny reservation.
SE and UK wondered why paragraph 2 of Article 13 of the 1995 Data Protection Directive had not been copied here. DE, supported by DK, HU, RO, PT and SI, stated that para. 1 should not only permit restrictions of the rights of data subjects but also their extension. For example, Article 20(2)(b) requires that Member States lay down 'suitable measures to safeguard the data subject's legitimate interests', which, when they take on the form of extended rights of access to information as provided for under German law in the case of profiling to asses creditworthiness (credit scoring), go beyond the Proposal for a Regulation.

392 AT reservation.

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

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

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

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

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

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

(g) the enforcement of civil law claims.

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

# CHAPTER IV

# CONTROLLER AND PROCESSOR[394]

## SECTION 1

## GENERAL OBLIGATIONS

*Article 22*

***Obligations of the controller***

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

2. (…)

2a. Where proportionate in relation to the processing activities[395], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

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

3. (…)

4. (…)

---

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

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

*Article 23*

***Data protection by design and by default***

1. (…) Having regard to available technology and the cost of implementation and taking account of *the nature, scope, context and purpose**s** of the processing* as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, including **data** minimisation[396] and pseudonymisation[397], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary[398] for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

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

3. (…)

4. (…)

---

396 **IT scrutiny reservation**.

397 DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. This debate will however need to take place in the context of a debate on pseudonymising personal data.
**PL: scrutiny reservation on provisions concerning pseudonymisation.**

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

*Article 24*

***Joint controllers***[399]

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

2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers.

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

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

*Article 25*

***Representatives of controllers not established in the Union***

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

2. This obligation shall not apply to:

   (a) (…); or

   (b) *processing which is* occasional[400] and *unlikely to result in a* (…) *risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing* (…); or

   (c) a public authority or body;

   (d) (…)

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

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

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

[400] HU, SE and UK reservation.

*Article 26*

***Processor***

1. (…).[401] The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…).

1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes[402].

1b. (…)[403].

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

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

---

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

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

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

(b) (…)

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

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

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

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

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

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

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

2a. Where a processor enlists (…) another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law*[404], in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

*2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or* an approved *certification mechanism pursuant to Article 39*[405] may be used as an element to demonstrate *sufficient guarantees referred to in paragraphs 1 and 2a*.

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

---

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

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

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2) [406].

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

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

4. (…)

5. (…)[407]

*Article 27*

***Processing under the authority of the controller and processor***

(…)

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

[407] COM reservation on deletion.

*Article 28*

***Records of categories of personal data processing activities***[408]

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

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

   (b) (…)

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

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

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

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

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

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

**408** AT scrutiny reservation.

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

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

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

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

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

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

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

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

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

(a) (…); or

(b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject such as (…) discrimination, identity theft or fraud, **unauthorized reversal of pseudonymisation**[409], financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or

[409] **AT, ES, IT, FR, NL, PL scrutiny reservation as regards pseudonymisation.**

5. (…)

6. (…)

*Article 29*

***Co-operation with the supervisory authority***

(…)

## SECTION 2

## DATA SECURITY

*Article 30*

***Security of processing***

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

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

2. (…)

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

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

3. (…)

4. (…)

*Article 31*

***Notification of a personal data breach to the supervisory authority***[410]

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

1a. The notification referred to in paragraph 1 shall not be required if a communication to the data subject is not required under Article 32(3)(a) and (b)[411].

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

---

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

**411** AT and PL thought this paragraph should be deleted.

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

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

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

(c) (…)

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

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

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

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

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

5. (…)

6. (….)[412]

[412] COM, supported by IT, reservation on deletion.

*Article 32*

***Communication of a personal data breach to the data subject***[413]

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

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

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

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

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

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

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

d. it would adversely affect a substantial public interest.

4. (…)

5. (…)

6. (…)[414]

[414] COM, supported by IT, reservation on deletion.

## SECTION 3

## DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

*Article 33*

***Data protection impact assessment*** [415]

1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high[416] risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, **unauthorized reversal of pseudonymisation**, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller (…)[417] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…).

---

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

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

**417** COM reservation on deletion.

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

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

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[418] are based that produce legal effects concerning data subjects or severely affect data subjects;

(b) processing of special categories of personal data under Article 9(1) (…)[419], biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale ;

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

(d) (…);

(e) (…)[420].

2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board. [421]

---

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

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

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

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

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

2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [422]

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1, the measures envisaged to address the risk including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned[423].

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment[424].

4. *The controller shall seek the views of data subjects or their representatives on the intended processing,* without prejudice to the protection of commercial or public interests or the security of the processing operations (…)[425].

---

422 CZ reservation.
423 FR scrutiny reservation.
424 HU thought this should be moved to a recital.
425 CZ and FR indicated that this was a completely impractical obligation; IE reservation.

5. (…) Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question[426], paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. (…)

7. (…)

*Article 34*

***Prior (…) consultation***[427]

1. (…)

2. The controller (…)[428] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high (…) risk in the absence of measures *to be taken by the controller* to mitigate the risk..

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

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

[428] COM and LU reservation on deleting processor.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may use any of its powers referred to in[429] Article 53 (…). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.

4. (…)

5. (…)

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

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

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

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

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

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

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

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

7. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure adopted by a national parliament or of a regulatory measure based on such a legislative measure which provide for the processing of personal data (…)[430].

7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[431].

8. (…)

9. (…)

[430] IE scrutiny reservation on deletion.
[431] SE scrutiny reservation.

## SECTION 4

## DATA PROTECTION OFFICER

*Article 35*

***Designation of the data protection officer***

1. The controller or the processor may, or where required by Union or Member State law shall,[432] designate a data protection officer (…).

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

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

4. (…).

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

6. (…)

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

---

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

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

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

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

11. (…)

*Article 36*

***Position of the data protection officer***

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

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

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

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

*Article 37*

***Tasks of the data protection officer***

1. The (…) data protection officer (…) shall have the following tasks:

(a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation and other Union or Member State data protection provisions (…);

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

(c) (…)

(d) (…)

(e) (…)

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

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

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

2. (…)

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

## SECTION 5
## CODES OF CONDUCT AND CERTIFICATION

*Article 38*

***Codes of conduct*** [433]

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

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

(a) fair and transparent data processing;

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

(b) the collection of data;

(bb) the pseudonymisation of personal data;

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

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

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

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

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

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

(f) (…).

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

1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory[434] monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

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

2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.

---

**434** CZ preferred this monitoring to be optional.

2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards[435].

3. Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards ,the European Data Protection Board shall submit its opinion to the Commission.

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

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

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

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

*Article 38a*

***Monitoring of approved codes of conduct***[436]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body[437] which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

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

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

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

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

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

---

**436** AT, LU scrutiny reservation.

**437** CZ, ES, LU are opposed to giving this role to such separate bodies. Concerns were raised, *inter alia*, on the administrative burden involved in the setting up of such bodies. Codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

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

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

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

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

*Article 39*

***Certification***[438]

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

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

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

2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2a. A certification pursuant to this Article shall be issued *by the* certification *bodies referred to in Article 39a, or where applicable, by the competent supervisory authority* on the basis of the criteria approved by the competent supervisory authority or, *pursuant to Article 57*, the European Data Protection Board[439].

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

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

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

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

*Article 39a*

***Certification body and procedure***[440]

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

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

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

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

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

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

[440] AT, FR, LU scrutiny reservation.

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

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

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

3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, *pursuant to Article 57*, the European Data Protection Board[441]. *In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies*.

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

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

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

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

6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation[442].

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 (…).

7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7[443].

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)[444].

---

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

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

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

# CHAPTER V

# TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[445] [446] [447] [448]

*Article 40*

***General principle for transfers***

(…)

[445] In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. FR and DE asked whether a transfer of data in the context of cloud computing or the disclosure of personal data on the internet constitutes an international transfer of data. DE also thought that the Regulation should create a legal framework for 'Safe Harbor-like' arrangements under which certain guarantees to which companies in a third country have subscribed on a voluntary basis are monitored by the public authorities of that country. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (FR, PL).

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

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

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

*Article 41*

***Transfers with an adequacy decision***[449]

1. A transfer of personal data to **(...)** a third country or an international organisation may take place where the Commission[450] has decided that the third country, or a territory or one ore more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

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

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…)[451], both general and sectoral, data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that third country or international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…)[452];

---

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

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

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

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

(b) the existence and effective functioning of one or more independent supervisory authorities[453] in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;

(c) the international commitments the third country or international organisation concerned has entered into, or other (…) obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data**.** [454]

2a. The European Data Protection Board shall give the Commission an opinion[455] for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.

---

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

454 DE suggested the following addition to point (c): "(c) the international commitments the third country or international organisation concerned has entered into, or other (…) obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data**.** ***International commitments must contain guarantees to be given by the third country that ensure an appropriate level of protection in particular when data are processed in one or several specific sectors. In particular, the third country must ensure effective data protection supervision by adequately involving European data protection supervisory authorities, and the data subjects must be provided with possibilities of effective legal redress.*** **The Presidency has added text to cover this aspect in recital 81.**

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

3. The Commission, after assessing the adequacy[456] of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…)**[457]. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies) mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2)[458].

3a. *Decisions adopted by the Commission on the basis of Article 25(6)* **(…)** *of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission*[459] Decision adopted in accordance with paragraph 3 or 5~~)~~[460].

---

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

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

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

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

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

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC[461].

5. The Commission may decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3)[462]. **(…)**

*5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.*

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44[463].**(…)**

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

8. (…)

---

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

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

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

*Article 42*

***Transfers by way of appropriate safeguards***[464]

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

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

   (oa) a legally binding and enforceable instrument between public authorities or bodies[465]; or

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

   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2)[466]; or

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

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

---

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

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

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

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

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

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

(b) (…)

(c) (…)

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

3. (…)

4. (…)

5. (…)

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

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority*[467]*. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission*[468] Decision adopted in accordance with paragraph 2[469].

*Article 43*

***Binding corporate rules***[470]

1. The competent supervisory authority shall *approve*[471] *binding corporate rules* in accordance with the consistency mechanism set out in Article 57 provided that they:

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

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

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

---

467 UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. IT was thought that this was contrary to the principle of accountability. DE emphasised the need of monitoring.

468 AT thought an absolute time period should be set.

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

470 NL thought it should be given a wider scope. BE and NL pointed to the need for a transitional regime allowing to 'grandfather' existing BCRs. NL asked whether the BCRs should also be binding upon employees. SI thought BCRs should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied. HU said that it thought that BCRs were used not only by profit-seeking companies but also by international bodies and NGOs.

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

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the *concerned* group and of each of its members;

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

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

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

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

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage[472];

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

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

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

(hh) the complaint procedures;

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

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

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph[473];

(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules[474]; and

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

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

---

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

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

3. (…)[475]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).[476]

*Article 44*

***Derogations for specific situations***[477]

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

(a) the data subject has explicitly[478] consented to the proposed transfer, after having been informed that such transfers may involve *risks* for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

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

---

475 NL, PL scrutiny reservation
SE reservation considering that implementing acts lack sufficient flexibility.

476 ES: scrutiny reservation

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

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

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

(d) the transfer is necessary for important reasons of public interest[479]; or

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

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

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

(h) the transfer, *which* is not large scale or *frequent*[480], is necessary for the purposes of legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and (…) based on this assessment adduced suitable safeguards[481] with respect to the protection of personal data.

---

479 DE remarked that the effects of (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties. IT reservation on the (subjective) use of the concept of public interest. HR suggested adding 'which is not overridden by the legal interest of the data subject'.

480 AT, ES, HU, MT, PL, PT and SI would prefer to have this derogation deleted as they think it is too wide; it was stated that data transfers based on the legitimate interest of the data controller and directed into third countries that do not provide for an adequate level of protection with regard to the right of the data subjects would entail a serious risk of lowering the level of protection the EU *acquis* currently provides for.)
**HU suggested as an alternative to deletion of point (h), that transfers based on Article 44(1)(h) must be subjected to a prior approval of the competent supervisory authority.**
DE and ES scrutiny reservation on the terms 'frequent or massive'. DE, supported by SI, proposed to narrow it by referring to 'overwhelming legitimate interest'. ES proposed to replace it by 'are small-scale and occasional'; UK asked why it was needed to add another qualifier to the legitimate interest of the transfer and thought that such narrowing down of this derogation was against the risk-based approach.

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

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

3. (…)

4. Points (a), (b), (c) and (h) of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers[482].

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

5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation[483]. Member States shall notify such provisions to the Commission[484].

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

6a. (…)

7. (…)

---

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

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

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

***Article 45***

*International co-operation for the protection of personal data*[485]

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;
   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[486];
   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;
   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. (…)

[485] PL thought (part of) Article 45 could be inserted into the preamble. NL, RO and UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI. NL thought this article could be deleted. ES has made an alternative proposal, set out in 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394.

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

# CHAPTER VI
# INDEPENDENT SUPERVISORY AUTHORITIES

## SECTION 1
## INDEPENDENT STATUS

*Article 46*

***Supervisory authority***

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

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

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

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them[487].

*Article 47*

***Independence***

1. Each supervisory authority shall act with complete independence in performing the duties[488] and *exercising* the powers entrusted to it in accordance with this Regulation.

---

**487** DE, FR and EE that thought that this paragraph could be moved to the final provisions.

**488** GR scrutiny reservation.

2. The member or members of each supervisory authority shall, in the performance of their duties and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody[489].

3. (…)[490]

4. (…)[491]

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

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

7. Member States shall ensure that each supervisory authority is subject to financial control[492] which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, annual budgets, which may be part of the overall state or national budget.

---

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

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

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

492 EE reservation.

*Article 48*

***General conditions for the members of the supervisory authority***

1. Member States shall provide that the member or members of each supervisory authority must be appointed (…) by the parliament and/or the government or the head of State of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure[493].

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

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the law of the Member State concerned[494].

4. (…)

5. (…)[495].

---

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

**494** COM reservation and DE scrutiny reservation on the expression "in accordance with the law of the Member States concerned". The question is whether this means that the Member States are being granted the power to define the duties further or whether the wording should be understood as meaning that only constitutional conditions or other legal framework conditions (e.g. civil service law) should be taken into account. DE and HU also suggest that rules in the event of death or invalidity be added (see, for example, Article 42(4) of Regulation (EC) No 45/2001) as well as referring to a procedure for the nomination of a representative in case the member is prevented from performing his or her duties. CZ, NO, SE see no need for paragraph 3

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

*Article 49*

***Rules on the establishment of the supervisory authority***

1. Each Member State shall provide by law for:

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

(b) the qualifications (…) required to perform the duties of the members of the supervisory authority[496];

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

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

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

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

(g) (…)[497].

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

---

[496] IE reservation: IE thought these qualifications need not be laid down in law.

[497] CZ, DE scrutiny reservation on deletion of this point.

*Article 50*

***Professional secrecy***

(…)

## SECTION 2

## COMPETENCE, TASKS AND POWERS

*Article 51*

***Competence***

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State. (…)
2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent[498]. In such cases Article 51a does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[499]. (…).

*Article 51a*

***Competence of the lead supervisory authority***

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

---

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

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

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

2b. In the cases referred to in paragraph 2a, the supervisory authority shall inform the lead supervisory authority without delay on this matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will deal with the case in accordance with the procedure provided in Article 54a, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

2c. Where the lead supervisory authority decides to deal with the case, the procedure provided in Article 54a shall apply. The supervisory authority which informed the lead supervisory authority may submit to such supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in paragraph 2 of Article 54a.

2d. In case the lead supervisory authority decides not to deal with it, the supervisory authority which informed the lead supervisory authority shall deal with the case according to Articles 55 and 56.

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

4. (…).

*Article 51b*

***Identification of the supervisory authority competent for the main establishment***

(…)

*Article 51c*

***One-stop shop register***

(…)[500]

*Article 52*

***Tasks*** [501]

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

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

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

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

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

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

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

[501] DE, IT, AT, PT and SE scrutiny reservation.

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

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

(d) conduct investigations on the application of this Regulation, including on the basis of a information received from another supervisory or other public authority;

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

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

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

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

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

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

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

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

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

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

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

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

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

2. (…)

3. (…).

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

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

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[502].

[502] DE and SE reservation: this could be left to general rules.

*Article 53*

***Powers***[503]

1. Each Member State shall provide by law that its supervisory authority shall have at least[504] the following investigative powers:

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

(aa) to carry out investigations in the form of data protection audits[505];

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

(b) (…)

(c) (…)

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

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

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

---

**503** DE, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, RO and UK) or opposed (DE, DK, and IE) to categorising the DPA powers according to their nature.

**504** RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules. COM and ES scrutiny reservation on 'at least' in paragraphs 1 and 1a.

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

1a. (…).

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

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

(b) to issue reprimands[506] to a controller or processor where processing operations have infringed provisions of this Regulation[507];

(c) (…);

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

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

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

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

(g) to impose an administrative fine pursuant to Articles 79 and 79a[508], in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.

---

506 PL scrutiny reservation.

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

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

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

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

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

(ab) to authorise processing referred to in Article 34(7a), if the law of the Member State requires such prior authorisation;

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

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

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

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

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

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

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

2. *The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.*[509]

3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and (…), where appropriate, to commence or engage otherwise in legal proceedings[510], in order to enforce the provisions of this Regulation[511].

4. (…)

5. (…)

*Article 54*

***Activity Report***

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

---

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

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

**511** DE thought para. 3 should be deleted.

# CHAPTER VII[512]

# CO-OPERATION AND CONSISTENCY

## SECTION 1

## CO-OPERATION

*Article 54a*

***Cooperation between the lead supervisory authority and other concerned supervisory authorities***

*513*

1. The lead supervisory authority (…) shall cooperate with the other concerned supervisory authorities in accordance with this article in an endeavour to reach consensus (…). The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other.

1a. The lead supervisory authority may request at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

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

---

**512** AT and FR scrutiny reservation on Chapter VII.

**513** CZ, CY, DE, EE, FR, FI, IE, LU, RO and PT scrutiny reservation.

3. Where any[514] of the other concerned supervisory authorities within a period of four weeks after having been consulted in accordance with paragraph 2, expresses a relevant and reasoned objection *to the draft decision*, the lead supervisory authority shall, if it does not follow the objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 57. (…)

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

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

4a. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other concerned supervisory authorities and the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

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

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

4bb. Where the lead supervisory authority and the concerned supervisory authorities are in agreement to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof[515], while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint and notify it on that complainant[516] and shall inform the controller or processor thereof. [517]

4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a and 4bb, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other concerned supervisory authorities.

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

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

---

515 Further to suggestions from HU and IE.

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

517 Further to suggestions from HU and IE.

*Article 54b*

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

(…)

*Article 55*

***Mutual assistance***[518]

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. (...)

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month[519] after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation (…).

---

**518** DE, SE and UK scrutiny reservation.

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

3. The request for assistance shall contain all the necessary information[520], including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

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

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute[521]; or

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

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request[522].

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means[523], using a standardised format.

---

520 EE and SE scrutiny reservation.

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

522 RO scrutiny reservation.

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

7. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances[524].

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure[525] on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57[526].

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months[527]. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57.

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)[528].

---

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

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

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

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

528 DE, IT, EE and CZ reservation.
SE, supported by CZ, reservation considering that implementing acts lack sufficient flexibility.

*Article 56*

***Joint operations of supervisory authorities***[529]

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

2. In cases where the controller or processor has establishments in several Member States or where a significant number of[530] data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in compliance with its own Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…) [531]

---

529 DE, EE, PT and UK scrutiny reservation.

530 COM reservation; IT, supported by FR and CZ suggested stressing the multilateral aspect.

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

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

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

3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State[532].

4. (…)

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

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

[532] UK reservation on paras. 3a, 3b and 3c.

## SECTION 2

## CONSISTENCY[533]

*Article 57*

***Consistency mechanism***[534]

1. For the purpose set out in Article 46(1a), the supervisory authorities shall co-operate with each other through the consistency mechanism as set out in this section[535].

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

(a) (…);

(b) (…);

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

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

---

533 IT and SI scrutiny reservation. DE parliamentary reservation and UK reservation on the role of COM in the consistency mechanism.

534 EE, FI and UK scrutiny reservation.

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

(cb) aims at approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to (…) paragraph 3 of Article 39a;

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

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

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

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

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

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

c) (…)

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

4. Any supervisory authority, the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

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

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

*Article 58*

***Opinion by the European Data Protection Board***[536]

1. (…)

2. (…)

3. (…)

[536] UK scrutiny reservation.

4. (…)

5. (…)

6. (…)

7. In the cases referred to in paragraphs 2 and 4 of Article 57, the European Data Protection Board shall issue an opinion on the subject- matter submitted to it provided it has not already issued an opinion on the same matter. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. This period may be extended by a further month, taking into account the complexity of the subject matter. Regarding the draft decision circulated to the members of the Board in accordance with paragraph 6 of Article 57, a member which has not objected within the period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft decision in accordance with paragraph 2 of Article 57.

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

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

9. Where the concerned supervisory authority informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph **3** of Article 57 shall apply.

10. (…)

11. (…)

*Article 58a*

***Decisions by the European Data Protection Board***[537]

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

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

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

3. In case the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board[538]. In case the members of the Board are split, the decision shall by adopted by the vote of its Chair.

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

5. (…)

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

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

7. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged shall adopt their final decision on the basis of the decision referred to in paragraph 1[539], without undue delay and at the latest by one month after the European Data Protection Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged, shall inform the European Data Protection Board of the date when its final decision is notified respectively to the controller or the processor and the data subject. The final decision of the concerned supervisory authorities shall be adopted under the terms of Article 54a, paragraph 4a, 4b and 4bb. The final decision shall refer to the decision referred to in paragraph 1 and shall specify that the decision referred to in paragraph 1 will be published on the website of the European Data Protection Board in accordance with paragraph 6. The final decision shall attach the decision referred to in paragraph 1.

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

*Article 59*

***Opinion by the Commission***[540]

(…)

*Article 60*

***Suspension of a draft measure***[541]

(…)

*Article 61*

***Urgency procedure***[542]

1. In exceptional circumstances, where a concerned supervisory authority considers that there is an urgent need to act in order to protect rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Article 57[543] or the procedure referred to in Article 54a, immediately adopt provisional measures intended to produce legal effects within the territory of its own Member State[544], with a specified period of validity. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the other concerned supervisory authorities, the European Data Protection Board and to the Commission.

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

---

540 COM and FR reservation on deletion.
541 COM and FR reservation on deletion.
542 DE scrutiny reservation.
543 HU remarked that it should be clarified whether provisional measures can be adopted pending a decision by the EDPB. The Presidency thinks that the reference to Article 57 makes it clear that this is indeed possible.
544 COM scrutiny reservation.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the European Data Protection Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

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

*Article 62*

***Implementing acts***

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

(a) (…)[545];

(b) (…);

(c) (…);

(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 57(5) and (6) and in Article 58(8).[546]

[545] COM reservation on deletion.

[546] SE, supported by CZ, reservation considering that implementing acts lack sufficient flexibility.

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

2. (…)

3. (…)

*Article 63*

***Enforcement***

(…)

**Section 3**

**European Data Protection Board**

*Article 64*

***European Data Protection Board***

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

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

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

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

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

*Article 65*

***Independence***

1. The European Data Protection Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 66 (…) and 67.[547]

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody[548].

*Article 66*

***Tasks of the European Data Protection Board***

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

(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(3) without prejudice to the tasks of national supervisory authorities;

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

---

**547** UK and SI scrutiny reservation.

**548** DE scrutiny reservation.

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

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a[549];

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

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

(cb) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4 of Article 39[550];

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

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

---

[549] DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.

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

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in paragraph 2 and on matters submitted pursuant to paragraph 4 of Article 57;

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

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

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

(h) (…);

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

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

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

*Article 67*

***Reports***

1. (…)

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

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1) as well as of the binding decisions referred to in paragraph 3 of Article 57.

*Article 68*

***Procedure***

1. The European Data Protection Board shall adopt binding decisions referred to in paragraph 3 of Article 57 in accordance with majority requirements set out in paragraphs 2 and 3 of Article 58a. As regards decisions related to the other tasks listed in Article 66 hereof, they shall be taken by a simple majority of its members.

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

*Article 69*

***Chair***

1. The European Data Protection Board shall elect a chair and two deputy chairs from amongst its members by simple majority[551](…)[552].

2. The term of office of the chair and of the deputy chairs shall be five years and be renewable once[553].

*Article 70*

***Tasks of the chair***

1. The chair shall have the following tasks:

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

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

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

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

---

551 IE proposal.
552 COM reservation on deletion.
553 COM scrutiny reservation.

*Article 71*

***Secretariat***

1. The European Data Protection Board shall have a secretariat, which shall be provided by the secretariat of the European Data Protection Supervisor (…).

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

1b. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation shall be organizationally separated from, and subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor[554].

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

2. The secretariat shall provide analytical[555], administrative and logistical support to the European Data Protection Board.

3. The secretariat shall be responsible in particular for:

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

[554] CZ reservation on last part of the task.
[555] UK suggested deleting "analytical".

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

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

(d) the translation of relevant information;

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

(f) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the European Data Protection Board.

*Article 72*

***Confidentiality***[556]

1. The discussions[557] of the European Data Protection Board shall be confidential.

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

---

556 DE, EE, ES, RO, PL, PT, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this. This article should be revisited once there is more clarity on the exact role and powers of the board, including the question whether the EDPS shall ensure the Secretariat.

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

# CHAPTER VIII

# REMEDIES, LIABILITY AND SANCTIONS[558]

*Article 73*

***Right to lodge a complaint with a supervisory authority***[559]

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single supervisory authority, in particular[560] in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation[561].

2. (…)

3. (…)

4. (…)

5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 74 (…)**.**

---

**558** AT, FR, EE, ES and RO scrutiny reservation.

**559** CY, CZ, LY, and SI scrutiny reservation.

**560** COM, BG, IT, SI and LU though that the data subject should be able to lodge a complaint with any DPA without limitation since the protection of personal data was a fundamental right.

**561** DE suggested adding "when its rights are not being respected".

*Article 74*

***Right to an effective[562] judicial remedy against a supervisory authority[563]***

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.[564].

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to *an effective* judicial remedy where the supervisory authority competent in accordance with Article 51 and Article 51a does not deal with a complaint or does not inform the data subject[565] within three months or any shorter period provided under Union or Member State law[566] on the progress or outcome of the complaint lodged under Article 73[567].

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

---

562 *Effectiv*e has been added, in line with Article 47 in the Charter. In particular recital 113 illustrates what an effective legal remedy means in this context: 'Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it'.

563 SI reservation. UK scrutiny reservation.

564 DE, supported by CZ, IE and SE, suggested adding: 'by which it is adversely affected'. FI thought that *concerning them* was too vague and suggested *addressed to them or:* (drafting is taken from Article 263 TFEU). However this criterion for ECJ litigation may not be necessarily be valid for remedies before national courts, the admissibility of which will be determined by national law.

565 FI and SE indicated that the right to a judicial remedy if an authority did not take action was unknown in their legal system. FI suggested a recital to solve this issue (footnote under recital 111).

566 SI indicated that under its law the DPA was obliged to reply within two months.

567 SE scrutiny reservation. NO wanted to delete paragraph 2 since a court review would endanger the independency of the DPA.

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

4. (…)

5. (…)[568]

*Article 75*

***Right to an effective judicial remedy against a controller or processor***[569]

1. Without prejudice to any available administrative or non-judicial remedy[570], including the right to lodge a complaint with a supervisory authority under Article 73, data subjects shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation. [571]

[568] COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.

[569] DE, PL, PT, SI and SK scrutiny reservation. ES reservation. FR, supported by BE, suggested to introduce a recital (new recital 117) stating that contractual clauses that do not respect Article 75 would be void. FR indicated that Facebook had been convicted in France for having inserted such a clause in a contract. **SK found that questions on recognition and enforcement of judgements should be resolved and text inserted into the GDPR.**

[570] SI wanted to delete *non-judicial remedy.*

[571] AT said that the possibility of parallel proceedings about the same object was not provided under its legal system and proposed to limit the possibility of a judicial remedy to cases where the DPA cannot take a decision. FR thought that it was necessary to clarify that the processor might be responsible independently of the controller, *e.g.* pursuant to Article 30 or according to a certification.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment (…)[572]. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor[573] is a public authority acting in the exercise of its public powers[574].

3. (…)

4. (…)

[572] In view of the concerns raised, the reference to national law has been kept only in recital 113.

[573] FR wanted to delete *processor*: in its opinion a processor cannot be a public authority.

[574] UK scrutiny reservation: found the second part of the paragraph unusual. DE, supported by PL and SI, suggested to add text in the end of the paragraph with a reference to the Brussels I Regulation indicating that the provisions of the present Regulation took precedence over the provisions of the Brussels I Regulation.

*Article 76* [575]

***Representation of data subjects***

1. The data subject shall have the right to mandate a body, organisation or association, *which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf* [576] and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf[577].

1a. (...)[578]

[575] DE, PT, RO and SI scrutiny reservation. CZ, EE, MT, NL, SI and UK thought this article was superfluous.

[576] NL had serious concerns with paragraph 1 because it feared that a system with class action like in the US would be introduced and pointed to the links with Articles 75 and 77. NL therefore suggested, supported by BE and BG, to add 'this body, organisation or association does not have the right to claim damages on his/her behalf', but mentioned that this text could go into a recital.

[577] DE parliamentary reservation; EE and FI reservation and HU scrutiny reservation. EE, supported by HU and SE, thought that the data subject could choose anybody to represent her/him so this drafting was a limitation so a reference to national law was needed. Support from SE. FI, supported by ES, suggested to add in the end of the paragraph 'in accordance with criteria laid down in national law'. FI also suggested to start paragraph 1 as follows: 'Any body ...may lodge a complaint when the data subject has mandated it, …behalf in accordance with national law. FI explained that this was to clarify that no body/organisation had an obligation to act which went too far for FI; support from ES that preferred to leave that for national law.

[578] FR asked for its reinsertion. BG welcomed its deletion.

**2.** Member States may[579] provide that any body, organisation or association referred to in paragraph 1, independently of a data subject's mandate (…)**,** shall have in such Member State the right to lodge a complaint with the supervisory authority competent in accordance with Article 73 **and** [580]**[581]** ~~**have the right to an effective judicial remedy against a supervisory authority in accordance with Article 74 or to an effective judicial remedy against a controller or a processor in accordance with Article 75**~~ **to exercise the rights referred to in Articles 73, 74 and 75**[582] if it considers that the rights of a data subject have been infringed as a result of the processing of personal data **that is not** in ~~**non**~~ compliance with this Regulation.

3. (…)

4. (…)[583]

---

**579** COM reservation. COM and FR wanted to replace *may* with *shall.* CZ, EE, ES, NL could in a spirit of compromise accept paragraph 2; NL on condition that *may* remained. BG, DE, DK**,** HU, EL, IE, MT also supported *may.* HU suggested to broaden the scope of the Article to cover all kinds of non-compliance of the Regulation. BG suggested in addition to set out, either in the body of the text or by referring to national law, a period of time in which the affected data subject would have the possibility to confirm his/her interest and to join the complaint or to withdraw it. In case there is no affected concrete data subject or he/she could not be identified, the complaint lodged will serve as a signal for the SA to start a check for a breach.

**580** COM said that the added value of the was that an organisation that had been recognised in on MS could mandate such an organisation in another MS.

**581** IE, RO, UK supported new paragraph 2. FR asked for the reinsertion of former paragraph 2. EL thought that is should be for national law to set out such possibilities. FR joined EL in that if the right for a body to lodge a complaint was not compulsory (shall) there was no need for the provision and the MS could set it out in their national law. BG wanted to introduce text allowing the data subject to confirm its interest in the action or withdraw its interest.

**582** **Aligned to the wording of paragraph 1.**

**583** COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.

*Article 76a*

***Suspension of proceedings***[584]

1. Where a competent court of a Member State has information[585] on proceedings concerning the same subject matter as regards processing **(...)** of the same controller or processor are pending in a court in another Member State, it shall[586] contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing (...) of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may[587] suspend[588] its proceedings.[589]

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

---

584 AT, BE, CY, DK, EE, ES, FI, FR, PL, PT, SE and SI scrutiny reservation. PL, supported by FI, wanted it to be explained what *same processing activities* thought: same scope or also related cases. ES thought that *lis pendens* necessitated the same persons, same proceeding, same object of dispute and same claim and that that could be difficult to establish.UK, supported by FR, cautioned against having a too prescriptive text, support from FR. SE thought that GDPR should not regulate *lis pendens*, but left to the DPAs and courts to decide. NO and FR asked how this text related to Regulation No 44/2001 and the Lugano Convention FI considered that it was necessary to have rules on this question in GDPR. MT found the text too prescriptive.

585 FR suggested to say *is informed* instead of *has information* to clarify that the parties had to inform the court.

586 LU supported by EL and MT, suggested to replace "shall" with "may". FR suggested to add *at the request of a party* clarifying that the court was not supposed to act of its own motion.

587 PL found it illogical that courts shall contact other courts in paragraph 1 but that they only *may* suspend proceedings. PL and CZ therefore preferred that the other courts were obliged to suspend their proceedings (shall and mot may) in paragraph 2.

588 PL and SK thought that it was difficult to force courts to stay proceedings waiting for another court to decide. HU supported by SK, asked how it was possible for a court to know that another case was going on elsewhere. HU asked how it would be established which court was first seized if several courts in several Member States were seized on the same day.

589 FR suggested adding in the end of the paragraph: *provided that such suspension respects the procedural rights of the parties to the proceedings.*

3. (…).

*Article 77*

***Right to compensation and liability***[590]

1. Any person who has suffered material or immaterial[591] damage[592] as a result of a processing which is not in compliance with this Regulation[593] shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Any controller **(…)** involved in the processing shall be liable for the damage caused by the processing which is not in compliance with this Regulation. A processor shall be liable for **~~violations~~ not complying with ~~of~~** this Regulation only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller.

---

**590** IE, PL and EL reservation. Several Member States (DE, NL and UK) have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. IT suggested specifying that these rules are to be applied according to national law, support from CZ, NL, RO and SI. COM thinks that it has to be left to ECJ to interpret these rules and concepts. FR scrutiny reservation; FR questioned the division of responsibilities and the link to Articles 24 and 25 and national law in this field as well as the principle of subsidiarity. IE asked from whom the data subject could seek compensation, since paragraphs 2 and 3 were contradictory. Nor UK liked the *joint* and s*eparately* responsibility and paragraphs 2 and 3 were contradictory. FI supported IE and UK and said that the processor had too much responsibility.

**591** DE, HU, NO, SE and SK suggestion.

**592** BE asked whether a violation of the principles of the Regulation was enough to constitute a damage or whether the data subject had to prove a specific damage (*obligation de moyens ou de résultat*). COM said that the data subject had to prove the damage.

**593** EL raised strong concerns that the notion of 'unlawful processing' as used in the1995 Directive were not repeated here and feared that this would lower the level of protection. EL further found the current wording of the GDPR too restrictive since national provisions and measures are not covered. EL therefore suggested inserting the following text in the first paragraph or in a chapeau: 'The application of the provisions of Article 77(1) and (2) cannot prejudice the application of national provisions in matters relating to tort, delicts and quasi-delicts.

3. ~~The controller or the processor~~ shall ~~be exempted from liability, (…) if~~ **they**~~(…) prove that they are not responsible~~ **in whole** ~~for the event giving rise to the damage.~~

**If a controller or processor proves that it is not in any way liable, in accordance with paragraph 2, for the event giving rise to the damage, it shall be exempted from providing compensation for the damage suffered as a result of processing that is not in compliance with this Regulation.**

4. *Where more than one controller or processor or a controller and a processor are involved in the same processing* and, **where they are** responsible for any damage caused by the processing**,** *in accordance with* ~~***the conditions set out in***~~ *paragraphs 2 and 3***,**each controller or processor shall be held (…) liable *for the entire damage***.**

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of liability for the damage in accordance with the conditions set out in paragraph 2.

6. *Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under national law of the Member State referred to in paragraph 2 of Article 75.*

*Article 78*

***Penalties***

(…)[594]

*Article 79*

***General conditions for imposing administrative fines***

1. Each supervisory authority shall **(...)**[595] ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a ***(…)*** *shall in each individual case be effective, proportionate and dissuasive.*[596]

2. **(…)**

[594] This Article was moved to Article 79b. Scrutiny reservation by SK, RO and PT.

[595] It was pointed out (FI) that the empowerment for Member States to provide for administrative sanctions and measures was already covered by Article 53(1b).

[596] Moved from paragraph 2. FI thought that paragraph 2 was not necessary since paragraph 2a provided concrete content for the general wording of paragraph 2.

2a. *Administrative fines shall*[597]*, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in* points (a) to (f**)** of paragraph 1b of *Article 53*[598]. When deciding whether to impose an administrative fine **(...)**[599] and [600]deciding on the amount of the administrative fine in each individual case due regard shall[601] be given **(...)** to the following:[602]

(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned as well as *the number of data subjects affected and the level of damage suffered by them*;

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

(c) **(...)**;

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

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

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

(g) **(…)**;[603]

---

597 CZ, FR, SE and UK suggested to change *shall* to *may.*

598 Some delegations thought that the corrective measures of Article 53 (1b) should be listed rather here.

599 Deleted further to FI suggestion.

600 Some delegations (EE, SK, PL) thought that aggravating circumstances should be distinguished from mitigating circumstances. SK suggested laying down exact thresholds (e.g. more than 2/3 of the maximum fine in case of aggravating circumstances).

601 UK suggested to insert *as appropriate.* DE was generally happy with the text since the list in was open and not all aspects needed to be considered. COM pointed at point (m) confirming that it was an open list.

602 PL and FR suggested that guidelines by the Board could be useful here or at least in a recital.

603 Deleted further to DK, ES, FR, FI and SI reservation.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement[604];

(i) in case measures referred to in ~~**point (b) and (c) of paragraph 1**~~ and points (a), (d), (e) and (f) of paragraph 1b of Article 53, have previously been ordered against the controller or processor concerned with regard to the same subject-matter[605], *compliance with these measures* ;

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39[606];

(k) (…);

(l) (…);

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

3. (…)[607]

3a. (…)[608]

3b. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State[609].

---

604 CZ and SE were concerned that this factor might amount to a violation of the privilege against self-incrimination.

605 IT thought this paragraph should refer more generally to previous incidents. DE and FR pleaded for its deletion.

606 CZ, FR, EE and SI reservation: DE pointed out that non-adherence to approved codes of conduct or approved certification mechanisms could as such not amount to a violation of the Regulation. IT found this point problematic and said that if the chapeau was reworded point (j) could be deleted.

607 COM reservation on deletion; linked to reservation on Article 79a.

608 COM reservation on deletion.

609 DE would prefer to rule out this possibility in the Regulation. ES thought it should be provided that no administrative fines can be imposed on the public sector. FR strongly supported paragraph 3b.

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

5. Member States may abstain from providing rules for administrative fines as referred to in paragraphs 1, 2 and 3 of Article 79a where their legal system does not provide for administrative fines and the infringements referred to therein are already subject to criminal sanctions in their national law by [date referred to in Article 91(2)], while ensuring that these criminal sanctions are effective, proportionate and dissuasive, taking into account the level of administrative fines provided for in this Regulation.[610]

   Where they so decide, Member States shall notify, to the Commission, the relevant parts of their criminal law[611].

---

**610** IE thought that the last part of the paragraph. from 'taking into account …' could go too far and limit the MS rights to legislate severer sanctions; it therefore suggested to delete that same part of the paragraph. Cion opposed IE and said that the last part was necessary, the sanctions should at least be in line with administrative fines.

**611** This paragraph builds upon a similar provision in Article 30(1) of the 2014 Market Abuse Regulation (EU) No 596/2014 of the European Parliament and the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, OJ 12.06.2014, L 173, p. 1. AT, HU scrutiny reservation. DE, DK, E, NL, EE and SE supported the text whereas FR, IE and PL could not accept it.. COM suggested text setting out that ' where national law of the MS don't provide for administrative sanctions ...' COM also suggested setting. DK thought that the legal basis (Article 16 TFEU) does not allow for the harmonisation of criminal law.

*Article 79a*

***Administrative fines***[612] [613]

1. The supervisory authority (…) may impose a fine that shall not exceed 250 000 EUR, or [614]in case of an undertaking 0,5 %[615] of its total worldwide annual turnover [616] of the preceding financial year, on a controller who, intentionally or negligently:

---

[612] DK reservation on the introduction of administrative fines in the text as administrative fines – irrespective of their level – raise constitutional concerns. DE, EE, ES, IE and PT scrutiny reservation. FI and SI reservation. COM reservation on replacing 'shall' by 'may'. DE wanted the risk-based approach to be made clearer. DE thought that proportionality was important because Article 79a concerned fundamental rights/rule of law and deemed it disproportionate that a supervisory authority could impose a fine that the data subject was unaware of. DE said that it was necessary to set out the fines clearly and that the one-stop shop principle did not allow for exceptions being set out in national law. IE thought e gravity of offences was not sufficiently illustrated, *e.g.* infringement in para. 3(m), which according to IE is the most serious one. FR reservation: the strictness of the text may impinge on the independence of the DPA. ES also wanted to give flexibility to the DPA.

[613] A majority of Member States (BE, CY DE, EE, ES, FI, IT, LV, LU, MT and NL) appear to be in favour of different scales of sanctions. COM referred to the Market Abuse Regulation with three levels of fines. DK, HU, IE, SE and UK were opposed to maintaining different sanctions scales. FR and PL did not favour it, but could accept it. SI said that it was impossible to have amounts in the Article. In contrast NL wanted to set out amounts.

[614] FI suggested to insert *if higher* to clarify that the higher amount is the maximum amount for sanctions, also valid for paragraphs 2 and 3.

[615] EE did not consider it appropriate to set out sanctions in percentage because the sanction was not predictable. PT considered that there should be minimum penalties for a natural person and that for SMEs and micro enterprises the volume of the business should not be looked at when applying the fines (this factor should only be applicable for multinationals). PL thought that administrative fines should be implemented in the same way in all MS. PL said that the fines should be flexible and high enough to represent a deterrent, also for overseas companies. ES saw practical problems with worldwide fines. UK noted that the levels of fines in the EP report were far too high.

[616] UK commented that *turnover* was used in competition law and asked whether the harm was the same here. EE asked how the annual turnover was connected to the sanction. SI thought that compared to competition law where the damage concerned the society as a whole, data protection concerned private infringements. COM said that both competition law and data protection concern economic values, whereas data protection protects values of the data subject. COM further said that the fines must be dissuasive and that it was necessary to refer to something, *e.g.* percentage but that it was also necessary with a sufficiently broad scope to take into account the specificities of the case. UK thought that *name and shame* would be a more efficient practice than fines. UK further said that high fines would entail two problems: they would be challenged in court more often and controllers might get less help to verify a potential breach. DE, supported by FR, thought that the fines set out in Article 79a were only the maximum level and that question of fines could be submitted to the Ministers in June JHA Council. COM agreed that the Article only set out maximum fines and that the companies themselves would provide the amounts of the turnover.

(a) does not respond within the period referred to in Article 12(2) to requests of the data subject;

(b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.

2. The supervisory authority **(…)** may impose a fine that shall not exceed 500 000 EUR, or in case of an undertaking 1% of its total worldwide annual (…) turnover of the preceding financial year, on a controller or processor who, intentionally or negligently:

(a) does not provide the information, or (…) provides incomplete information, or does not provide the information [timely or] in a [sufficiently] transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;

(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 (…);

(c) does not erase personal data in violation of the right to erasure and 'to be forgotten' pursuant to Article 17(1)(a), 17(1)(b), 17(1)(d) or 17(1)(e);

(d) (…)

(da) processes personal data in violation of the right to restriction of processing pursuant to Article 17a or does not inform the data subject before the restriction of processing is lifted pursuant to Article 17a(4);

(db) does not communicate any rectification, erasure or restriction of processing to each recipient to whom the controller has disclosed personal data, in violation of Article 17b;

(dc) does not provide the data subject's personal data concerning him or her (…) in violation of Article 18;

(dd) processes personal data after the objection of the data subject pursuant to Article 19(1) and does not demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims;

(de) does not provide the data subject with information concerning the right to object processing for direct marketing purposes pursuant to Article 19(2) or continues to process data for direct marketing purposes after the objection of the data subject in violation of Article 19(2a);

(e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;

(f) does not or not sufficiently[617] maintain the documentation pursuant to Article 28 and Article 31(4).

(g) (…)

3. The supervisory authority **(…)** may impose a fine that shall not exceed 1 000 000 EUR or, in case of an undertaking, 2 % of its total worldwide annual turnover of the preceding financial year, on a controller or processor who, intentionally or negligently:

(a) processes personal data without a (…) legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;

(b) (…);

(c) (…);

(d) does not comply with the conditions in relation to (…) profiling pursuant to Article 20;

(da) does not (…) implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 (…) and 30;

[617] IE, supported by SI, pointed it that a number of the terms used here (such as "sufficiently", "timely" and "incomplete") were so vague that they were not compatible with the *lex certa* principle. DE agreed with IE and added that it was a problem of objective of the provisions: on the one side the need for the controller to know what the rules are and on the other side the flexibility for the DPA.

(db) does not designate a representative in violation of Article 25;

(dc) processes or instructs the processing of personal data in violation of (…) Articles 26;

(dd) does not alert on or notify a personal data breach or does not [timely or] completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;

(de) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);

(e) (…);

(f) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

(g) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;

(h) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).

(i) (…)[618]

(j) (…).

3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.[619]

[618] IT wanted to reinstate failure to cooperate with the DPO. IE thought that this was a subjective infringement.

[619] PL and FR wanted to keep paragraph 3a.

4. **(…)** [620]

*Article 79b*

***Penalties***[621]

*1. For infringements (…)of this Regulation* in particular for infringements which are not subject to administrative fines pursuant to (…) *Article 79a Member States shall*[622] *lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (…). Such penalties shall be effective, proportionate and dissuasive.*

*2. (…).*

*3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.*

---

620 CZ, DE, HU, NL and RO reservation. NL that thought that guidelines from the EDPB could solve the problems on the amounts. CZ wanted to delete the paragraph and thought that the DPA could set out the amounts.

621 AT, DE, DK, ES, FR, PL and PT and SK scrutiny reservation. COM explained that infringements not listed in Article 79a were those under national law, referred to in Chapter IX, for example infringements in employment law and relating to freedom of expression. In that way Article 79b is complementary to the list in Article 79 and does not exclude other penalties. IT thought it was better to delete the Article but lay down the possibility to legislate at national level. FR reservation on the imposition of criminal penalties. DE in favour of referring *expressis verbis* to criminal penalties. IE concerned that the provision would apply to infringements of the freedom of expression laws. In the same vein EE raised concerns because EE doesn't have laws on the freedom of expression.

622 HU reservation.

# CHAPTER IX
# PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

*Article 80*

***Processing of personal data and freedom of expression and information***

1. The national law of the Member State shall (…) reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For *the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression*, Member States shall[623] provide for exemptions or derogations from the provisions in Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation and consistency)[624] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (…).

---

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

[624] BE, DE, FR, IE and SE had requested to include also a reference to Chapter VIII. This was opposed to by COM. The Presidency points out that in case the freedom of expression prevails over the right to data protection, there will obviously no infringement to sanction. Where an infringement is found to have place, the interference with the freedom of expression will have to taken into account as an element in the determination of the sanction. This application of the proportionality principle should be reflected in Chapter VIII.

*Article 80a*

***Processing of personal data and public access to official documents*** [625]

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

*Article 80aa*

***Processing of personal data and reuse of public sector information***

*Personal data in in public sector information held by a public authority or a public* body or a private *body* for the performance of a task carried out in the public interest *may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject* in order to reconcile the reuse of such official documents and public sector information with *the right to the protection of personal data pursuant to this Regulation*[626].

[625] SK and PT scrutiny reservation.

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

*Article 80b* [627]

***Processing of national identification number***

Member States may determine the specific conditions for the processing of a national identification number or any other identifier of general application. In this case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

*Article 81*

***Processing of personal data for health -related purposes***

(…)[628]

*Article 81a*

***Processing of genetic data***

(…)[629]

627 DK, PL, SK scrutiny reservation.

628 See Article 9(2)(g),(h), (hb) and (4) which enshrine the basic idea, previously expressed in Article 81, that sensitive data may be processed for purposes of medicine, health-care, public health and other public interests, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

629 See Article 9(2)(ha) and (4) which enshrine the basic idea, previously expressed in Article 81a, that genetic data may be processed, e.g. for medical purposes or to clarify parentage, subject to certain appropriate safeguards based on Union law or Member State law. This text is not part of the partial general approach which the Council is asked to agree at its meeting of 4 December 2014 and will be subject to further scrutiny at technical level.

*Article 82*

***Processing in the employment context***[630]

1. Member States may by law or by collective agreements, provide for more specific[631] rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. (…)

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. Member States may by law determine the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee[632].

*Article 82a*

***Processing for purposes of social protection***

(…)

630 **AT reservation**

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

632 This paragraph may need to be looked at again in the context of the discussions on Articles 7 and 8 for consent. COM, PL, PT scrutiny reservation.

*Article 83*

***Derogations applying to processing of personal data for archiving, scientific, statistical and historical purposes***

1. Where personal data are processed for scientific, statistical[633] or historical purposes Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18 and 19[634], insofar as such derogation is necessary for the fulfilment of the specific purposes.

1a. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may, subject to appropriate safeguards for the rights and freedoms of the data subject, provide for derogations from Articles 14a(1) and (2), 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 and 53 (1b)(d) and (e), insofar as such derogation is necessary for the fulfilment of these purposes[635].

1b. In case a type of processing referred to in paragraph**s** 1 and 1a serves at the same time another purpose, the derogations allowed for apply only to the processing for the purposes referred to in those paragraphs.

2. The appropriate safeguards referred to in paragraphs 1 and 1a shall be laid down in Union or Member State law and be such to ensure that technological and/or organisational protection measures pursuant to this Regulation are applied to the personal data (…), to minimise the processing of personal data in pursuance of the proportionality and necessity principles, such as *pseudonymising the data,* unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled within reasonable means.

3. (…).

---

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

**634** NL and DK proposed adding a reference to Article 7. SI supported this as far as scientific processing is concerned. PL suggested deleting the reference to Article 19.

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

*Article 84*

***Obligations of secrecy*** [636]

1. (…) Member States may adopt specific rules to set out the (…) powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects under Union or Member State law or rules established by national competent bodies to an obligation of professional secrecy**,** other equivalent obligations of secrecy or to a code of professional ethics supervised and enforced by professional bodies, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

*Article 85*

***Existing data protection rules of churches and religious associations***[637]

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1, shall be subject to the control of an independent supervisory authority which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

---

**636** DE and UK scrutiny reservation.

**637** MT, NL, AT and PT reservation.

# CHAPTER X

# DELEGATED ACTS AND IMPLEMENTING ACTS[638]

*(1) Article 86*

***Exercise of the delegation***

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in (…) Article 39a(7) (…) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in (…)Article 39a(7) **(…)** may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

---

**638** COM reservation on the deletion of empowerments for delegated acts or implementing acts including the recitals (129), (130) and (131).
SI: scrutiny reservation.
AT considered that for lack of sufficient legal arrangements in the Regulation itself, delegated and implementing acts can have a function, where needed in combination with guidelines of the EDPB.. Therefore, AT can accept the Commission proposal on delegated acts as regards the Articles 6(5), 8(3), 9(3), 26(5), 39(7), 39(8), 41(3), 41(5) and the EP suggestions in relation to the Articles 43(4), 43(4) and 79, and the Commission proposal on implementing acts in relation to Articles 18(3), 26(2b), 31(6), 30(4), 32(6), 38(4), 42(2) subparagraphs (b) and (c), 43(4), 55(10) and 61(1d).

5. A delegated act adopted pursuant to (…)Article 39a(7) (…) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

*Article 87*

***Committee procedure***

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

## CHAPTER XI

## FINAL PROVISIONS

*Article 88*

***Repeal of Directive 95/46/EC***

1. Directive 95/46/EC is repealed.

2. [639]References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

[639] UK: reservation. UK considers that the current drafting does not work for the purposes it is intended to achieve. Propose to redraft article : "References to particular parts or provisions in the repealed Directive are to be construed as references to the equivalent provisions in the Regulation [..]."
IT: scrutiny reservation
IE pointed to the practical problems of repeal of Directive 95/46/EC and replacement by the new GDPR. DE, CZ and NL queried whether a list existed of legislative acts that would be affected by such replacement. Cion indicated that a transitional period of 2 years is foreseen.

*Article 89*[640] [641]

***Relationship to and amendment of Directive 2002/58/EC***[642]

1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.[643]

---

640 FI suggested to insert a related recital: "In relation to this Regulation, the information security measures that are meant to protect the transmission and confidentiality of communications can be regulated nationally under the Article 4 and 5 of the Directive 2002/58/EC and under the Article 13a of the framework Directive 2002/21/EC."

641 CZ, DK, IE, IT, FI, NL, UK wanted to keep 89 with deletion of para 2 (as in the text now).
BG expressed preference for deleting art 89 but could be flexible.
FR, NL scrutiny reservation, inter alia s regards the phrase "the same objective". FR did not necessarily want to delete para 2.
PL, SI: scrutiny reservation.
DE requested clarification of Cion why article 89 was proposed.
AT wanted to delete art 89 so that Directive 2002/58/EC would be covered by art 88.

642 AT, BE, DK, FR, IT: scrutiny reservation concerning the consistent application of the e-Privacy Directive and the GDPR. In reaction, Cion indicated that the e-Privacy Directive complements Directive 95/46/EC. The e-Privacy Directive will need to be adapted after adoption of the GDPR.
FR queried why only a reference was made to the e-Privacy Directive and not also to fi the e-commerce Directive.
AT, supported by HU and HR, suggested to add: "When in doubt, this Regulation is applicable and not Directive 2002/58/EC when more beneficial for the data subject."

643 FR was dissatisfied with the drafting of this Article and meant that it would be unclear for the controller what rules that would be applicable to him/her (how could they know about the *objective* of a certain provision), this Regulation or the e-privacy Directive. NL supported FR that a clarification was necessary. **BE scrutiny reservation on the links between this Regulation and the e-privacy Directive.**

2 (…)

*Article 89a*

***Relationship to previously concluded Agreements***

*International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked*[644].

*Article 90*

***Evaluation***

1. The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals.[645].

2. In the context of these evaluations the Commission shall examine, in particular, the application and functioning of the provisions of Chapter VII on Co-operation and Consistency.

3. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The reports shall be made public.

---

644 Cion reservation based on strong legal doubts on the legality of such proposal. Cion refers to recital (79).
AT, HU: reservation and IT, PL, RO and UK scrutiny reservation considering that all relevant international agreements need to be checked if they are in compliance and they can only be adapted in cooperation with the third country contracting parties.

645 DE, supported by FI, wanted to specify other aspects that in particular needed to be evaluated.DE suggested to add: - the functioning of the provisions of chapter III and their effects in practice on the data subjects and controllers; and
- the functionality of the provisions of this Regulation with regard to new technological developments.
UK, supported by Cion, wanted the phrase on OSS to be in a separate paragraph.
PL: scrutiny reservation wanting the EDPB to be involved in the evaluation.

4. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

*Article 91*

***Entry into force and application***

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from [*two years from the date referred to in paragraph 1*][646].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

| | |
|---|---|
| *For the European Parliament* | *For the Council* |
| *The President* | *The President* |

---

**646** CZ, DE, FR scrutiny reservation about the moment of applicability of the regulation on data individual processing operations so as to provide legal certainty and avoid bureaucracy. CZ, FI, HU, SE wanted a longer transitional period for the Regulation to become applicable than the foreseen 2 years. DE referred to Article 41(3a) on adequacy decisions that would remain valid until amended etc. and meant that this should also apply to decisions made by national authorities based on such decisions. DE noted that in three places (also Articles 42(5)(b) and 89a)) in the GDPR sunset clauses were inserted but not here. In the same vein FR raised concerns for the processing itself and found it exaggerated that such processing would be invalid only because they did not comply with the GDPR. NL and CZ supported DE and FR and NL asked for specific provisions for this to create legal certainty. Cion replied to DE and FR that the objective of the GDPR was a reform of the existing data protection rules: this implied that the standards and rules of the GDPR must be followed from the day of its application. Cion opposed a general sunset clause and recalled that, where appropriate, a specific clause ensuring continuity was foreseen in Article 41(3a) and 42(5)(b).
Furthermore Cion stressed that a 2 years' transitional period is special for applicability of a regulation.