COUNCIL OF THE EUROPEAN UNION

Brussels, 28 January 2013

5702/13

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 2
JAI 47
MI 44
DRS 17
DAPIX 6
FREMP 3
COMIX 40
CODEC 155

NOTE

from:	Presidency
to:	Working Party on Data Protection and Exchange of Information
No. prev. doc.:	15703/4/12 REV 4 DATAPROTECT 122 JAI 752 DAPIX 137 MI 678 FREMP 131 DRS 121 COMIX 608 CODEC 2555 16525/12 DATAPROTECT 132 JAI 819DAPIX 145MI 753FREMP 141 DRS 131 CODEC 2744 16529 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745
Subject:	Implementation of risk-based approach in the General Data Protection Regulation

1. At the JHA Council meeting in December 2012, DAPIX was instructed to continue to work on concrete proposals to implement a strengthened risk-based approach in the text of the draft Regulation. This Presidency paper seeks to take account of Member State concerns set out specifically in replies to the questionnaire on administrative burdens (15703/4/12 REV 4) and more generally during DAPIX discussions on Chapters III and IV.

2. The purpose of the Presidency paper is to provide a concrete basis for incorporating such a risk-based approach, in particular in Chapter IV (Controller and Processor) (see annex 1), and in certain articles in Chapter III (Rights of the Data Subject) (see annex 2).

3. Annex 1 contains proposals for significant changes to several important articles in Chapter IV, especially articles 22, 23, 26, 28, 30, 31, 33, 34 and 35. The objective is to incorporate a risk-based approach, clarify and streamline the text and to drop certain provisions with limited value-added (articles 27 and 29) and others which would have enabled the Commission to adopt delegated acts and implementing acts, e.g. paragraph 4 of article 22; paragraph 3 of article 23 and paragraph 9 of article 34.

4. Annex 2 contains proposals for significant changes to several important articles in Chapter III, including articles 12, 14 and 15. The objective of these changes is to ensure effective and efficient exercise of data subject rights, while improving certainty and transparency. It is proposed to drop certain provisions which are no longer required due to restructuring of the text (articles 11 and 13) and others which would have enabled the Commission to adopt delegated acts and implementing acts, e.g. paragraphs 7 and 8 of article 14; paragraphs 3 and 4 of article 15.

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

6. The proposals set out in articles 17, 18, 20 and 21 of Chapter III will be examined at a later stage.

7. While the focus in this paper is on certain articles in Chapter III and Chapter IV, the Presidency recognises that a risk-based approach to implementation may be considered appropriate in certain other cases. These cases can also be discussed at a later stage.

8. The Presidency intends to report to the JHA Council meeting on 7/8 March on the progress being made in developing concrete proposals for implementing a strengthened risk-based approach in the draft Regulation.

CHAPTER IV
CONTROLLER AND PROCESSOR[1]
SECTION 1
GENERAL OBLIGATIONS

Article 22

Responsibility of the controller[2]

1. **Taking into account the nature, scope and purposes of the processing and the risks for the fundamental rights and freedoms of data subjects,** the controller shall (…) implement appropriate measures to **[**ensure and**]**[3] be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[4].

---

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

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

3 The Presidency shares the view of those Member States that question the feasibility of a result obligation; this is linked to the content of Article 5(f).

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

2. The controller shall, where required pursuant to this Regulation[5], **take appropriate** measures for:

(a) **retaining** details of the arrangements, contracts or other legal acts provided for in Articles 24(1) and 26(2)[6] and the documentation pursuant to Article 28;

(b) implementing the data security **and confidentiality** requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33[7];

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2) **and 42(6)**;

(e) designating a data protection officer pursuant to Article 35(1)[8].

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

(a) appropriate data protection policies by the controller;

(b) mechanisms to ensure that the time limits established for the erasure of personal data are observed[9].

---

5 Clarification further to DE remark.

6 Further to FR suggestion:

7 FR, LT and RO scrutiny reservation: FR thinks there is lack of legal certainty in this regard and that in particular the link with Article 33 should be clarified.

8 LT scrutiny reservation. FR thought this should be a closed list and proposed to add a subparagraph (f) in which reference would be made to Articles 24 and 26(2)

9 Moved from Article 17.

3. The controller shall implement mechanisms to **[**ensure **and]**[10] **be able to demonstrate (…)** verification of the effectiveness of the measures referred to in paragraphs 1 **to 2a**. (…)[11] [12].

4. **(…)**

Article 23

Data protection by design and by default[13]

1. Having regard to the state of the art and the cost of implementation and taking account of the risks for fundamental rights and freedoms of individuals posed by the nature, scope or purpose of the processing, [14] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself[15], implement (…) technical and organisational measures **(…)** appropriate to the activity being carried on and its objectives[16] **, including the use of pseudonymous data,** in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of **(…)** data subject**s**.[17]

---

10 See footnote 3.

11 FI, FR, IT, SE and DE expressed doubts on systematically using external auditors. BE and CZ pleaded for the deletion of the entire paragraph.

12 Second sentence moved to amended recital 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 [ensure and] be able to demonstrate the compliance of each processing operation with this Regulation. If proportionate, the verification of the obligations of the controller may be carried out by independent internal or external auditors.'

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

14 Further to SE suggestion.

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

16 ES proposal.

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

2. The controller shall[18] implement appropriate[19] **measures** for ensuring that, by default, only (…) personal data (…) which are necessary[20] for each specific purpose of the processing are processed**; (…) this applies to the** amount of **(…)** data **collected**, (...) the **period** of their storage and their accessibility[21]. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals[22].

3. **(…)**

[4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

---

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

19 SE suggestion.

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

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

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

Article 24

Joint controllers [23]

1. (…)[24] Joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a[25], by means of an arrangement between them[26] unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject[27].

2. The data subject may exercise **his or her** rights under this Regulation in respect of and against each of the joint controllers[28].

---

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

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

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

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

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

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

Article 25

Representatives of controllers not established in the Union[29]

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union[30].

2. This obligation shall not apply to:

   (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41[31]; or

---

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

30 SI reservation.

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

(b) an enterprise employing fewer than 250 persons; unless the processing it carries out, involves high risks for the fundamental rights and freedoms of individuals, taking account of its characteristics, the type of data or the number of persons it concerns [32]; or

(c) a public authority or body[33]; or

(d) a controller offering only occasionally goods or services to data subjects residing in the Union[34].

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[35].

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

---

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

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

34 ES, GR, IT and LT thought that this criterion in itself could not be sufficient to determine the applicability of the obligation to appoint a representative. DE and SK thought that this scenario was not covered by Article 3(2) and that at any rate the term 'occasionally' required further discussion.

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

Article 26

Processor[36]

1. Where personal data are processed on behalf of the controller, the controller shall be responsible for **[**ensuring**]**[37] compliance with data protection rules[38] and (…) shall use only a processor providing sufficient guarantees[39] to implement appropriate technical and organisational measures **(…)** in such a way that the processing will meet the requirements of this Regulation (…)[40].[41]

2. [Where the processor is not part of the same group of undertakings as the controller[42],] the carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, **the** nature and purpose of the processing, **the** type of data and **categories** of data subjects[43] or other legal act[44] binding the processor to the controller and stipulating in particular that the processor shall:

---

36 CZ reservation: this article should be deleted. Several delegations (DE, FR IT, LU, NL, SI, SK and UK) pointed to the difficulties in distinguishing the roles of controllers and processors, in particular in the context of cloud computing, where the controller often can not exercise (full) control over the way in which the processor handles the data and thought the proposed provision did not reflect the realities of cloud computing. DE thought the provision needed to be re-examined to see to what extent it is applicable to and meaningful for existing and emerging procedures and services in the health sector, in particular the processing of pseudonymised data or data rendered unintelligible and the administration of medical file systems under the patient's control ('google health', 'health vault'). BE also referred to the case of the data subject who is himself controller. The concerns raised need to be addressed in the context of a broad debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. Until such debate has taken place in DAPIX, no fundamental changes are made to the text as far as this relationship is concerned.

37 See footnote 3.

38 DE proposal for a basic rule. Cf. recital 62.

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

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

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

42 Further to NL and SE remark that a processor who is part of the same concern as the controller would not necessarily act on the basis of a contract.

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

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

(a) process the personal data only on instructions from the controller (…)[45], unless required to do so by Union or Member State law law to which the processor is subject[46];

(b) (…)[47];

(c) take all (…) measures required pursuant to Article 30[48];

(d) determine the conditions for enlisting another processor (…)[49];

(e) as far as (…) possible**, taking into account** the nature of the processing[50], assist the controller in[51] responding to requests for exercising the data subject's rights laid down in Chapter III;

(f) determine the extent to which[52] the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) **(…)** not process the personal data **further after the completion**[53] **of the processing specified in the contract or other legal act,** unless there is a requirement to store the data[54] under Union or Member State law **to which the processor is subject**;

---

45 DE wondered whether this requirement was feasible in the context of social media.
46 Addition to ensure consistency with Article 27 (as pointed out by BE, FR, ES, SI and UK).
47 This was deleted; all confidentiality requirements have now been inserted in Article 30.
48 UK and IE thought there was an overlap with Article 30.
49 IE and UK thought this overlapped with other parts of the Regulation (Article 26,(2)(a) and 30). BE thought the requirement should be deleted and DE thought it should at least have been limited to establishment of contractual relationships. SK scrutiny reservation.
50 FR wanted to know what was meant by this phrase.
51 Further to DE proposal.
52 DE and UK remarked that the processor may not always be able to provide such assistance.
53 SI queried when processing was 'ended'.
54 Further to NL and SE suggestion.

(h) make available to the controller (…)[55] all information[56] necessary to **demonstrate** compliance with the obligations laid down in this Article.

3. The controller and the processor shall retain in writing or in an equivalent form[57] the controller's instructions and the processor's obligations referred to in paragraph 2.

4. (…)[58].

4a. **The processor shall inform the controller if the processor considers that an instruction by the controller would breach the Regulation[59].**

5. **(…)**

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

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

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

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

[59] Further to DE proposal.

Article 27

Processing under the authority of the controller and processor

(…) [60]

Article 28

Documentation [61]

1. Each controller **(…)**[62] and, if any, the controller's representative, shall maintain documentation of all **categories of** processing activities[63] under its responsibility.

2. **This** documentation shall contain (…)[64] the following information:

   (a) the name and contact details of the controller, any joint controller or processor, and of the **controller's** representative, if any;

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

   [(c) the purposes of the processing [including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)][65];

---

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

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

62 Several delegations (BE, DE) thought the processor should not have cumulative obligations with the controller. ES and UK pointed out that the impact of cloud computing needed further reflection. There needs to be a broader debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. Until such debate has taken place in DAPIX, no fundamental changes have been made to the text as far as this relationship is concerned.

63 DE and BE thought it might have been preferable to confine the scope of this obligation in the same way as Article 18 of the 1895 Data Protection Directive: 'any wholly or partly automatic processing operation or set of operations intended to serve a single purpose'.

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

65 BE and UK proposed to delete this part. COM is opposed thereto.

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

(e) the **(…)** categories of recipients of the personal data **(…)**;

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

(g) a general indication of the time limits for erasure of the different categories of data[66];

(h) **(…)**

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

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

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

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

(d) where applicable, the categories of transfers of personal data to a third country or an international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards.

[66] ES pointed out that this would not always be possible. FR and SI thought that the word 'general' should be deleted.

3. **Upon request, t**he controller [and the processor] and, if any, the controller's representative, shall make the documentation available (…) to the supervisory authority[67].

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

(a) (…)[68]

(b) (…)[69].

(c) categories of processing **activities** which are unlikely **to represent risks for ,** the fundamental rights and freedoms of data subjects[70] **by virtue of the nature, scope or purposes of the processing**;

5. **(…)**

6. **(…)**

---

67 SI wondered why the data subject was not mentioned here. COM stated this information of the data subject is covered by the general principles.

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

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

70 Proposal inspired by Article 18(2) of the Data Protection Directive, in order to take account of delegations (DE, FR, and PT) that thought that the proposed exceptions were not well-founded and that risk-based exceptions would be preferable.

Article 29

Co-operation with the supervisory authority

(…)[71]

SECTION 2
DATA SECURITY AND CONFIDENTIALITY

Article 30

Security and confidentiality of processing[72]

1. **Having regard to the state of the art and the costs of their implementation and taking into account the nature, scope and purposes of the processing and the risks for the fundamental rights and freedoms of data subjects,** the controller and the processor[73] shall implement appropriate technical and organisational measures**, including the use of pseudonymous data,** to ensure a level of confidentiality and security appropriate to these risks (…).

2. (…) [74].

---

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

[72] Several delegations (DE, FR, and IE) thought that more clarity was required as to what kind of risks for which actors were concerned. DE regretted the text of Article 17 of the 1995 Data Protection Directive had not been followed more closely. PT would have hoped for a more ambitious text.

[73] Several delegations thought that the controller should have the main responsibility (NO) and have a clearer division of responsibilities (UK). These concerns need to be addressed in the context of a broad debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. As this debate still needs to take place in the DAPIX Working Party, no fundamental changes have been made to the text as far as this relationship is concerned.

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

2a. **The obligation of confidentiality on any person acting under the authority of the controller or the processor shall continue to have effect after the termination of their activity for the controller or processor**

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations

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

Article 31

Notification of a personal data breach to the supervisory authority[75]

1. In the case of a personal data breach which is likely to adversely affect the **fundamental rights and freedoms** of data subjects[76], the controller shall without undue delay and, where feasible, not later than 72[77] hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51[78]. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours[79].

2. **(…)** The processor shall alert and inform the controller immediately after the establishment[80] of a personal data breach[81].

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

   (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

---

75 SI scrutiny reservation. Several delegations (CZ, DE, FR, PT, SI and UK) also highlighted the potential conflict between the proposed notification duty and the privilege against self-incrimination, as a notification might eventually lead to sanctions against the controller making the notification. The Presidency agrees that this topic needs to be further investigated, also in the light of the ECHR case law (see e.g. the judgment of 17 December 1996, *Saunders v. United Kingdom*).

76 Inspired by E-Privacy Directive (Article 4(3)) in order to take account of the concern voiced by several delegations (BE, ES, IT, LU, PL, PT, SE and SK) thought that the text should distinguish between minor and grave personal data breaches in order to avoid disproportionate administrative burdens both on data controllers and on data protection authorities

77 Further to criticism by BE, CZ, DE, ES, GR, MT, NL, LU, PT, SE, SI and UK. DE would have preferred no specific time limit. COM scrutiny reservation.

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

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

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

81 The Commission highlighted the importance of this obligation, in particular in the context of cloud computing.

(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 consequences of the personal data breach[82];

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

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach[83] .

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

4. The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken[84]. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

[5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

[82] BE thought this was impossible.
[83] Copied from (c). Further to remarks by FR, GR and LU.
[84] AT and FR queried what was the retention period for this documentation.

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

Article 32

Communication of a personal data breach to the data subject[85]

1. When the personal data breach is likely to adversely affect the **fundamental rights and freedoms** of the data subject, the controller shall (…)[86] 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).

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

[86] The Presidency agrees with AT, PT and SE that there is no valid reason why the data subject should always be informed after the DPA. Therefore this part has been deleted.

3. Notwithstanding paragraph (1), the communication of a personal data breach to the data subject shall not be required if the controller (…)[87] has implemented appropriate technological protection measures[88] and **(…)** those measures were applied to the data **affected by** the personal data breach. Such technological protection measures shall **include those that** render the data unintelligible[89] to any person who is not authorised to access it[90]**, such as encryption or the use of pseudonymous data**[91].

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

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

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

---

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

88 PL thought this required further clarification.

89 DE thought this required further clarification.

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

91 The Presidency proposes a new recital 68a to accompany this text:
"*The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data and using pseudonymous data*."

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

1. Where **the** processing, **taking into account the nature, scope or purposes of the processing, is likely to** present specific[92] risks **for** the **fundamental** rights and freedoms of data subjects **(…)**, the controller [or the processor acting on the controller's behalf][93] shall, prior to the processing[94], carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

1a. Paragraph 1 shall not apply where a data protection officer has been designated in accordance with Article 35(4).

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

(a) a systematic and extensive evaluation **on a large scale** of personal aspects relating to **(…)** natural person**s (…)**, which is based on automated processing and on which decisions[95] are based that produce legal effects concerning **(…) data subjects** or significantly affect **data subjects**;

---

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

93 The Presidency thinks the reference to the processor need to be revisited in the context of a broad debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. Until such debate has taken place in DAPIX, the Presidency has not made any fundamental changes to the text as far as this relationship is concerned.

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

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

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

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale[96];

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

(e) other **operations where (…)** the **competent** supervisory authority **considers that the processing is likely to present specific risks for the fundamental rights and freedoms of data subjects**[97].

2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board. [98]

2b. Prior to the adoption of the list the supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union. [99]

---

96 BE and FR asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale',

97 BE suggested deleting this subparagraph.

98 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2.

99 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks **for fundamental** rights and freedoms of data subjects, the measures envisaged to address the risks, 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[100].

4. (…)[101]

5. Where the controller is a public authority or body and where the processing results from a legal obligation[102] pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law **or the law of the Member State to which the controller is subject**, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[103].

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

---

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

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

102 BE, CH, PT and SE suggested adding 'by Union or Member State law'. The Presidency does not deem this necessary as it already flows from Article 6 (3).

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

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

Article 34

Prior authorisation and prior consultation[104] [105]

1. (…)[106]

2. The controller [or processor acting on the controller's behalf][107] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that **the** processing **is** likely to present a high degree of specific risks[108].

(…)

---

[104] The Presidency suggests the possibility of an Amended recital 74 on the following lines: "*Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their rights, identity theft, discrimination, significant financial loss or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. The supervisory authority should respond to the request for consultation in a defined period, during which the controller or processor shall not commence processing activities. The absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its duties and powers laid down in this Regulation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards*".

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

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

[107] BE and SI were opposed to mentioning the processor here. The Presidency thinks the reference to the processor need to be revisited in the context of a broad debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. Until such debate has taken place in DAPIX, the Presidency has not made any fundamental changes to the text as far as this relationship is concerned.

[108] IE and SE scrutiny reservation on the concept of a high degree of specific risks.It was pointed out that such assesments might be time-consuming.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a **maximum** period of 6 weeks following the request for **consultation**[109] **(…)** make appropriate recommendations to the data controller [or processor][110]. **This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.**

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

4. **(…)**

5. **(…)**

6. **When consulting the supervisory authority pursuant to paragraph 2,** the controller [or processor][111] shall provide the supervisory authority[112], on request, with the data protection impact assessment provided for in Article 33 and any (…) information **requested by** the supervisory authority **(…)**.

---

[109] BE suggestion.

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

[111] BE was opposed to mentioning the processor here. The Presidency thinks the reference to the processor need to be revisited in the context of a broad debate on the respective roles of the controller vis-à-vis the processor, inter alia in the context of cloud computing. As this debate still needs to take place in the DAPIX Working Party, the Presidency has chosen so far not to make any fundamental changes to the text as far as this relationship is concerned.

[112] The data protection impact assessment is already provided to the DPA under paragraph 2(a).

7. Member States shall consult the supervisory authority **during** the preparation of **(…)** legislative **or regulatory** measure**s, or schemes based on such measures, which provide for the processing of personal data which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing;** in order to ensure compliance of the intended processing with this Regulation **such measures may concern the activities of public authorities and bodies, including those relating to health, employment and social security.**

[8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.]

9. **(…)**

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer[113]

1. The controller and the processor shall designate a data protection officer **(…)** where:

   (a) the processing is carried out by a public authority or body; or

   [(b) the processing is carried out by an enterprise employing 250 persons or more[114]; or

   (c) the core activities of the controller or the processor consist of processing **activities** which, **represent risks for the fundamental rights and freedoms of data subjects by virtue of the nature, scope or purposes of the processing** [115]][116].

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer[117].

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.

---

113 SI reservation. AT scrutiny reservation. Several Member States (BE, DK, EE, ES, LT, PL, SE, SI and UK) thought this should not be required in all cases; reference was made in particular to the impossibility to appoint a DPO in all public authorities. It was also stated that the cost of appointing a DPO could be too high, especially for smaller entities in the public, but also in the private sector. A substantial number of Member States (BE, CZ, FR, IT, NL, LV, LT, UK) thought that the function of DPOs should be a self-regulatory one without legally defined tasks and competencies. DE, BG and NO were in favour of the mandatory appointment of a DPO.

114 This criterion was criticised by BE, MT and PT as it did not relate to the quantity or quality of the data processed. DE thought the number of employees should be much lower, as under the proposed criterion only 0.2 % of all cases would be covered.

115 BE and CZ scrutiny reservation: unclear what is meant.

116 The Presidency would welcome further contributions on the scope of this provision.

117 DE thought that there might be cases where one data protection officer might not be enough for large groups of undertakings. SI queried whether this would not endanger the independence of the DPO.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer 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. The **(…)** level of expert knowledge shall be **appropriate to the processing activities of** the controller or the processor.

6. (…)[118].

7. **(…) The data protection officer shall be designated** for a period **appropriate to the processing activities of the controller or processor**. **(…)**. 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**[119], be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of **his or her** duties[120].

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

9. **Upon request,** the controller or the processor shall **make available** the name and contact details of the data protection officer 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.

---

[118] Moved to Article 36, new paragraph 4, for systematic reasons.

[119] Presidency suggestion in order to allay concerns (DE, DK, GR, ES, FR, HU, IT, LV, SE, UK) regarding the interference with national labour law.

[120] BE proposed to replace the latter part of the sentence by a reference to positions expressed by the DPO in his/her function.

[11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.]

Article 36

***Position of the data protection officer*[121]**

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 and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37. These means shall be adapted to the size and needs of the organisation of the controller or processor[122].

3. The controller or processor shall ensure that the data protection officer acts in an independent manner with respect to the performance of his or her duties and tasks[123] and does not receive any instructions **regarding** the exercise of the**se** function**s**. The data protection officer shall directly report to the **highest level of management**[124] of the controller or the processor[125].

---

121 COM clarified that its proposal for Article 36 and 37 were inspired by Regulation 45/2011.

122 BE suggestion.

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

124 BE suggested replacing this by ' highest level'.

125 BE suggested adding 'The data protection officer must ensure confidentiality of information obtained while performing his or her tasks, in particular as regards to information relating to complaints and information relating to the data processing activities of the controller or processor'. The Presidency believes this is already covered by the general confidentiality duty it has now inscribed in Article 30.

4. **The data protection officer may fulfill other tasks and duties. The controller shall ensure that any such tasks and duties do not result in a conflict of interests**[126].

Article 37

Tasks of the data protection officer

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

   (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity **(…)**

   (b) to monitor the implementation and application of this Regulation and of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising[127] and training of staff involved in the processing operations, and the related audits;

   (c) (…);

   (d) (…);

   (e) (…);

   (f) (…)[128];

   (g) to monitor the response 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[129];

---

126 Moved from Article 35 (6). DE was opposed to this as these requirements were irrelevant to the functional independence of the DPO. UK also thought this was too prescriptive. Presidency endeavoured to redraft this paragraph in order to make it less prescriptive.

127 Further to PL suggestion.

128 DK, GR SE, SI and UK thought this list was much too detailed. In response to this, the Presidency suggests deleting subparagraphs (c) to (f) as these are all covered by (a) (and (b).

129 DE suggested deleting this subparagraph as a DPO should not be a tool of the DPA.

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative[130].

2. **(….)**

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct [131]

1. The Member States, the supervisory authorities 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**, in particular in relation to:

   (a) fair and transparent data processing;

   (b) the collection of data;

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

   (d) requests of data subjects in exercise of their rights;

   (e) information and protection of children;

   (f) transfer of data to third countries or international organisations[132];

[130] FR suggested adding an obligation to draft an annual report on his activities, but the Presidency wonders whether this is not too heavy an obligation.

[131] DE and SI stated that this article should not apply to the public sector.

[132] NL queried whether this also covered the transfer to processors in 3rd countries.

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75[133].

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts[134].

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission[135].

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

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

---

133 SI reservation.

134 Based on national experiences, DE was sceptical as to the chance of success of this mechanism. IT and SE queried how to make the outcome binding.

135 DE, IE, ES, PT remarked that the DPAs should be involved. ES thought that the Commission need not necessarily be involved. SI suggested giving a role to the EDPB.

Article 39

Certification[136]

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of **(…)** specifying the criteria and requirements **to be taken into account** for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. 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).

---

136 CZ thought this Article should be deleted. DE, ES, FR, IT, NO and PT took a more favourable view, but thought the drafting was amenable to improvement. FR thought the terminology used was unclear. BE, SI and NL thought certification should take place mainly on a voluntary basis. COM indicated that this certification model would indeed take place on a voluntary basis.

CHAPTER III
RIGHTS OF THE DATA SUBJECT[137]

SECTION 1

TRANSPARENCY AND MODALITIES

Article 11

Transparent information and communication[138]

1. (….)[139]

2. (…)[140].

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

[138] SI reservation. Whilst delegations generally expressed support for the principle of transparency, many (DE, ES, EE, FI, MT, NL, NO, PL, PT, SE and UK) voiced concerns about the structure (the rights of the data subject should be spelled about before defining the obligations of the controllers), its relationship to other articles (11, 12, 14) and its indiscriminate application to all data controllers regardless of their size.

[139] The Commission argued that this provides a legal basis for a general transparency policy rather than the provision of information to individuals. AT, CZ, DE, ES, IE, SE and UK argued that there are not sufficient arguments for maintaining such a vaguely worded obligation, non-compliance of which is liable to sanctions. Therefore paragraph 1 was deleted.

[140] Moved to Article 12 (1).

Article 12

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

1. The controller shall[141] take appropriate measures to provide any information referred to in Article 14, 14 a and 20(4) and any communication under Articles 15 to 19 and 32[142] relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language, (…)[143] in particular **where** addressed specifically to a child. The information shall be provided in writing[144], **or** where appropriate, electronically **or by other means**[145].

1a[146]. The controller shall **facilitate data subject requests under** Articles 15 to 19 (…)[147]. Where personal data are processed by **electronic** means[148], the controller shall also provide means for requests to be made electronically[149].

---

141 NL proposes to insert 'having regard to the state of the art, the cost of the implementation, the risks of the processing and the nature of the data to be protected'.

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

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

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

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

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

147 This sentence was deleted at the suggestion of DE, as the concept of 'mechanisms for facilitating' was very vague and not appropriate for a legally binding text. UK thought the whole paragraph should be deleted.

148 ES and DE pointed out that there should be no causal link between the automatic processing of data and the possibility to make requests in an electronic form. DE therefore proposed to limit this to cases where the data processor communicates electronically. Therefore the condition was inserted that data must have been collected by automated means. CZ, ES and UK were opposed to this and thought this requirement was not technology neutral. CZ thought the form of communication should be agreed between the data controller and data subject.

149 SI and DE thought that the exact content of the obligations was not clear enough, in particular what the controller was supposed to do within the one-month period. ES proposed adding

2. The controller shall provide the information referred to in Article **15** and 20(4) and **information** on action taken **on a request under Articles 16** to 19[150] **to** the data subject without undue delay and at the latest within one month of receipt of the request[151] (…). This period may be extended for a further two months when necessary[152]**, taking into account the complexity of the request and the number of requests**[153]. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.

3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject **without delay and at the latest within one month of receipt of the request** of the reasons for not taking action[154] and on the possibility of lodging a complaint to a supervisory authority (…)[155].

'Where considered useful, all the information may be documented in the form of policies and manuals of procedure, to facilitate its understanding and handling'.

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

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

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

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

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

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

4. **I**nformation **provided under Articles 14, 14a and 20(4) and any communication under Articles 15 to 19 and 32**[156]**shall be provided** free of charge[157]. Where requests from a data subject are (…)[158] **unfounded or** manifestly excessive, in particular because of their repetitive character[159], the controller (…) may decline the request[160]. In that case, the controller shall bear the burden of **demonstrating the unfounded or** manifestly excessive character of the request.[161]

4a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject[162].

5. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4].

6. (…)

---

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

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

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

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

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

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

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

Article 13

Rights in relation to recipients

(...)[163]

SECTION 2

INFORMATION AND ACCESS TO DATA

Article 14

Information to the data subject <u>where the data are collected from the data subject</u>[164]

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

   (a) the identity and the contact details of the controller and, if any, of the controller's representative<u>; the controller may</u>[165] <u>also include the contact details</u> of the data protection officer<u>, if any</u>;

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

---

[163] This Article was moved to Article 17b.

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

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

1a. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with any further information necessary to **ensure** fair and transparent processing[166], having regard to the specific circumstances in which the personal data are processed, such as:

(a) the envisaged period for which the personal data will be stored[167];

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

(c) the recipients or categories of recipients of the personal data[168];

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

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

(f) the right to lodge a complaint to a supervisory authority (…)[169];

(…)

(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data[170].

---

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

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

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

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

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

2. (…)

3. (…)

4. (…)

5. Paragraphs 1 and 2 shall not apply where and insofar as the data subject already has the information (…).

6. (…)

7. **(…)**

8. **(…)**

Article 14 a

Information where the data have not been obtained from the data subject

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

   (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may[171] also include the contact details of the data protection officer, if any

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

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

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

(a) the categories of personal data concerned;

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

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

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

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

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

(g) the origin of the personal data[172], unless the data originate from publicly accessible sources[173].

3. The controller shall provide the information referred to in paragraphs 1 and 2[174]:

(a) **(…)** within a reasonable period[175] after **obtaining the data**, having regard to the specific circumstances in which the data are processed, or

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

---

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

173 DE, FR, FI, SI and UK pleaded for an exception for publically available data.

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

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

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

(a) the data subject already has the information[176]; or

(b) the provision of such information [in particular when processing personal data for historical, statistical or scientific purposes[177]], proves impossible or would involve a disproportionate effort[178]. **In such cases** the controller **shall** take appropriate measures to protect the data subject's legitimate interests[179], **for example by using pseudonymous data**[180]; or

(c) **obtaining** or disclosure is expressly laid down by Union or Member State[181] law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests.

(d) [where the data originate from publicly available sources][182]; or

(e) where the data must remain confidential in accordance with a legal provision or on account of the overriding justified interests of a third party[183].

---

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

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

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

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

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

181 Further to DE suggestion.

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

183 Further to DE proposal.

5. **(…)**

6. **(…)**

Article 15

Right of access for the data subject[184]

1. [185]The data subject shall have the right to obtain from the controller at reasonable intervals[186], on request, confirmation as to whether or not personal data **concerning him or her** are being processed. Where such personal data are being processed, the controller shall provide **to the data subject the personal data undergoing processing and** the following information:

   (a) the purposes of the processing;

   (b) (…)

   (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries[187];

   (d) the envisaged[188] period for which the personal data will be stored;

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

---

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

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

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

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

188 FR empahasisd the need of providing an exception to archives.

(f) the right to lodge a complaint to a supervisory authority (…)[189] [190];

(g) where the personal data are not collected from the data subject[191], any available information as to their source[192];

(h) in the case of measures referred to in Article 20, knowledge of the logic involved in any automatic data processing[193], the significance and envisaged consequences of such processing[194]

2. (…)[195]

3. **(…)**

4. **(…)**

[5. The rights provided for in Article 15 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met][196].

---

189 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.

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

191 DE proposal.

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

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

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

195 This paragraph was deleted. BE, CH, CZ, DE, ES and UK could not see how the first sentence differs from the obligation under paragraph 1(g). It thinks that the second sentence is covered by the penultimate sentence of Article 12 (1).

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

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[197]

1. **(…)** The data subject shall have the right[198] to obtain from the controller the rectification of personal data **concerning him or her** which are inaccurate. Having regard to the purposes for which data were processed,[199] the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…)[200] statement[201].

2. [The rights provided for in Article 16 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.][202]

---

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

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

199 Further to UK suggestion.

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

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

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

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19
Right to object[203]

1. The data subject shall have the right to object, on **reasoned** grounds relating to his or her particular situation, at any time to the processing of personal data **concerning him or her** which is based on points **(…)**, (e) and (f) of Article 6(1)[204]. **In such cases the personal data shall no longer be processed** unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject[205].

---

203 SI and SK scrutiny reservation.

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

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

2. Where personal data are processed for direct marketing[206] purposes, the data subject shall have the right to object free of charge at any time[207] to the processing of personal data **concerning him or her** for such marketing. This right shall be explicitly **brought to the attention of** the data subject (…)[208]. **Information concerning this right shall** be **presented** clearly **and separately** from any other information[209] [210].

[206] FR and UK under lined the need to have clarity regarding the exact content of this concept, possibly through a definition of direct marketing.

[207] IT proposal.

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

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

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

3. Where an objection is upheld[211] pursuant to paragraphs 1 and 2, the controller shall no longer (…)[212] process the personal data concerned except for the establishment, exercise or defence of legal claims[213].

4. [The rights provided for in Article 19 do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met[214]].

_____

[211] GR queried what happened pending the resolution of an objection.

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

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

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