Council of the European Union

Brussels, 16 March 2015
(OR. en)

7084/15

LIMITE

DATAPROTECT 31
JAI 169
MI 159
DRS 23
DAPIX 39
FREMP 50
COMIX 114
CODEC 336

Interinstitutional File:
2012/0011 (COD)

NOTE

From:	Presidency
To:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	15395/14 DATAPROTECT 165 JAI 860 MI 965 DRS 167 DAPIX 167 FREMP 202 COMIX 604 CODEC 2222
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Chapter III and VIII

Following the discussions at the DAPIX meetings of 9-11, 24, 29-30 April and 13 -14 May 2013 relating to Chapter III and of 23-24 September and 28-29 October 2013 relating to Chapter VIII and in light of the partial general approach on Chapter II, VI and VII reached at the JHA Council meeting on 13 March 2015, the Presidency has made some changes to the text of Chapter III and VIII, which are highlighted in the Annex in **bold underlined.**

Chapter III in its entirety was last discussed under the Irish Presidency and Chapter VIII in its entirety under the Lithuanian Presidency. Article 17 on the right to be forgotten in light of the Google case was discussed under the Italian Presidency (11289/1/14 REV 1), Article 20 on profiling (10617/14) and Article 18 on data portability (10614/14) were discussed under the Hellenic Presidency. Article 21 as well as the corresponding recital 59 were part of the partial general approach on the flexibility of the public sector that was reached in December 2014. Recitals 111-113 were part of the partial general approach on the One-Stop Shop.

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

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

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

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

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

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

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

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

53a) Inasmuch as the removal of links from the list of internet search results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst the data subject's rights protected by those articles should override, as a general rule, the interest of internet users, that balance may in specific cases depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having access to that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

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

54aa)[1] *However* **the right to be forgotten should be balanced with other fundamental rights. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. This may lead to the result that the personal data has to be maintained** *for exercising the right of freedom of expression, when required by law, for* **archiving purposes in the public interest or for** *historical, statistical and scientific (...) purposes, for reasons of public interest in the area of public health* **or social protection**, or **for the establishment, exercise or defence of legal claims**.

In order to exercise the right to be forgotten, the data subject may address his request to the controller without prior involvement of a public authority, such as a supervisory or judicial authority, without prejudice to the right of the data subject to lodge a complaint or initiate court proceedings against the decision taken by the controller. In these cases it should be the responsibility of the controller to apply the balance between the interest of the data subject and the other interests set out in this Regulation.

[1] This part is moved from the last part of recital 53.

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

55) To further strengthen the control over their own data (…), where the processing of personal data is carried out by automated means, the data subject should also be allowed to transmit the personal data concerning him or her, which he or she has provided to a controller, in a commonly used and machine-readable format to another controller.
This right should apply where the data subject provided the personal data based on his or her consent or in the performance of a contract. It should not apply where processing is based on another legal ground other than consent or contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of a**n** official duty vested in the controller.

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

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

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

58) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her and taken which is based solely on automated processing, *which produces legal effects concerning him or her* or significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' intended to create or use a profile, that is a set of data characterising a category of individuals to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements~~;~~. However, decision making based on such processing, including profiling, should be allowed when authorised[2] by Union or Member State law to which the controller is subject, including for fraud and tax evasion[3] monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention, to express his or her point of view, to get an explanation of the decision reached after such assessment[4] and the right to contest the decision.

Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.

---

2 BE suggested adding ' or recommended', with regard to e.g. ECB recommendations.
3 Further to MT suggestion.
4 Further to PL suggestion.

58a) The creation and the use of a profile, i.e. a set of data characterising a category of individuals that is e applied or intended to be applied to a natural person as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.

_____

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

112) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects. Such a body, organisation or association should have the right to lodge, independently of a data subject's complaint, a complaint where it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.

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

Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints[5]. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation.

Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[6], whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the European Data Protection Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.

(114) (…)

(115) (…)

---

5 GR reservation.

6 Case C-314/85

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

117) (…).

118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law[7].

118a) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation No 1215/2012 should not prejudice the application of such specific rules[8].

118b) In order to strengthen the enforcement of the rules of this Regulation, penalties and administrative fines[9] may be imposed for any infringement of the Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. The imposition of penalties and administrative fines should be subject to adequate procedural safeguards in conformity with general principles of Union law and the Charter of Fundamental Rights, including effective judicial protection and due process.

---

7 COM scrutiny reservation.

8 COM and DE scrutiny reservation.

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

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

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

CHAPTER III

RIGHTS OF THE DATA SUBJECT[10]

SECTION 1

TRANSPARENCY AND MODALITIES

Article 11

Transparent information and communication

1. (…)

2. (…)

Article 12

Transparent information, communication and modalities for exercising the rights of the data subject[11]

1. The controller shall take appropriate measures to provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language[12]. The information shall be provided in writing, or where appropriate, electronically or by other means.

1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 19[13]. (…)

10 General scrutiny reservation by UK on the articles in this Chapter.
11 DE, SE, SI and FI scrutiny reservation.
12 COM reservation on deletion.
13 SI and UK thought this paragraph should be deleted.

2. The controller shall provide the information referred to in Articles 14a and 15 and information on action taken on a request under Articles 16 to 19 to the data subject without undue delay and at the latest within one month of receipt of the request[14] (…). This period may be extended for a further two months when necessary, taking into account the complexity of the request and the number of requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.

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

4. Information provided under Articles 14 and 14a (…) and any communication under Articles 16 to 19 and 32 shall be provided free of charge. Where requests from a data subject are *manifestly* unfounded or excessive[15], in particular because of their repetitive character, the controller (…) may refuse to act on[16] the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request[17].

---

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

15 PL thought that the criterion of 'manifestly excessive' required further clarification, *e.g.* through an additional recital.

16 NL scrutiny reservation: avoid that this gives the impression that public authority cannot refuse to consider request by citizen.

17 IT scrutiny reservation.

4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

5. (…)

6. (…)

Article 13

Rights in relation to recipients

(...)

SECTION 2

INFORMATION AND ACCESS TO DATA

Article 14

Information to be provided where the data are collected from the data subject[18]

1[19]. Where personal data relating to a data subject are collected from the data subject, the controller shall (…), at the time when personal data are obtained, provide the data subject with the following information:

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

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

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

[19] HU thought the legal basis of the processing should be included in the list.

1a. In addition to the information referred to in paragraph 1, the controller shall[20] provide the data subject with such further information [21]necessary to ensure fair and transparent processing in respect of the data subject[22], having regard to the specific circumstances and context in which the personal data are processed[23]:

(a) (…);

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

(c) the recipients or categories of recipients of the personal data[24];

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

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data (…)[25];

---

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

21 CZ suggested adding the word 'obviously'.

22 FR scrutiny reservation.

23 COM reservation on deletion of the words 'such as'.

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

25 The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE.

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

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

(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as **whether the data subject is obliged to provide the data and of** the possible consequences of failure to provide such data[26];

(h) the existence of **automated decision making including** *-profiling referred to in Article 20(1) and (3) and information concerning* (…) *the* ***processing****, as well as the significance and the envisaged consequences of such* ***processing*** *for the data subject.* [27]

1b. Where the controller intends to process the data in accordance with Article 6(4) for another purpose than the one for which the data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 1a.

2. (…)[28]

3. (…)

4. (…)

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

[26] CZ, DE, ES and NL reservation.
[27] SE scrutiny reservation.
[28] HU reservation on the deletion of this paragraph.

6. (…)

7. (…)

8. (…)

Article 14 a

Information to be provided where the data have not been obtained from the data subject[29]

1[30]. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

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

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

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context[31] in which the personal data are processed (…):

(a) the categories of personal data concerned;

(b) (…)

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

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

---

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

30 HU thought the legal basis of the processing should be included in the list.

31 ES, IT and FR doubts on the addition of the words 'and context'.

(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 **(…)**;

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

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

(g) the origin of the personal data, unless the data originate from publicly accessible sources[32];

*(h) the existence of **automated decision making including** profiling referred to in Article 20(1) and (3) and information concerning (...) the **processing**, as well as the significance and the envisaged consequences of such **processing** for the data subject.*[33]

3. The controller shall provide the information referred to in paragraphs 1 and 2[34]:

(a) within a reasonable period 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.

---

32 COM and AT scrutiny reservation.

33 PL asks for the deletion of the reference to 'logic'.

34 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.

3a **Where the controller intends to process the data in accordance with Article 6(4) for another purpose than the one for which the data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.**

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

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

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing[35]; in such cases the controller shall take appropriate measures to protect the *data subject's* **rights and freedoms and** legitimate interests[36]; or

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests[37]; or

(d) where the data originate from publicly available sources[38]; or

(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person[39].

---

35 COM scrutiny reservation.

36 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.

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

38 COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.

39 COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.

5. (…)

6. (…)

Article 15

Right of access for the data subject[40]

1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge[41] (…) confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed access to the data and the following information:

   (a) the purposes of the processing[42];

   (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[43];

   (d) where possible, the envisaged[44] 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;

---

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

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

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

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

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

(f) the right to lodge a complaint to a supervisory authority (…)[45] [46];

(g) where the personal data are not collected from the data subject, any available information as to their source[47];

(h) in the case of **automated decision making including profiling** referred to in Article **20(1) and (3)**, knowledge of the logic involved[48] in any automated data processing as well as the significance and envisaged consequences of such processing[49].

1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer[50].

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

2. Where personal data supplied by the data subject are processed by automated means and in a structured and commonly used format, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject in that format to the data subject[51].

---

45 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.

46 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.

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

48 PL reservation on the reference to 'logic': the underlying algorithm should not be disclosed. DE reservation on reference to decisions.

49 NL scrutiny reservation. CZ and FR likewise harboured doubts on its exact scope.

50 FR and UK scrutiny reservation on links with Chapter V

51 COM, ES and FR reservation: they thought this was too narrowly drafted. DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy. DE scrutiny reservation on relation to paragraph 1.

2a. The right to obtain a copy referred to in paragraphs 1b and 2 shall not apply where such copy cannot be provided without disclosing personal data of other data subjects [52]

3. (…)

4. (…)

5. **(…)**[53]

[52] DE, supported by UK, referred to the danger that data pertaining to a third party might be contained in such electronic copy.

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

SECTION 3

RECTIFICATION AND ERASURE

Article 16

Right to rectification[54]

1. (…) The data subject shall have the right[55] to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…) statement.

2. **(…)**[56]

[54] DE and UK scrutiny reservation.

[55] UK suggested to insert the qualification ' where reasonably practicable' UK also suggested inserting the qualification 'where necessary'.

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

Article 17

Right to be forgotten and to erasure[57]

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

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

[57] DE, EE, PT, SE, SI, FI and UK scrutiny reservation. EE, FR, NL, RO and SE reservation on the applicability to the public sector. Whereas some Member States have welcomed the proposal to introduce a right to be forgotten (AT, EE, FR, IE); other delegations were more sceptical as to the feasibility of introducing a right which would go beyond the right to obtain from the controller the erasure of one's own personal data (DE, DK, ES). The difficulties flowing from the household exception (UK), to apply such right to personal data posted on social media were highlighted (BE, DE, FR), but also the impossibility to apply such right to 'paper/offline' data was stressed (EE, LU, SI). Some delegations (DE, ES) also pointed to the possible externalities of such right when applied with fraudulent intent (e.g. when applying it to the financial sector). Several delegations referred to the challenge to make data subjects active in an online environment behave responsibly (DE, LU and UK) and queried whether the creation of such a right would not be counterproductive to the realisation of this challenge, by creating unreasonable expectations as to the possibilities of erasing data (DK, LU and UK). Some delegations thought that the right to be forgotten was rather an element of the right to privacy than part of data protection and should be balanced against the right to remember and access to information sources as part of the freedom of expression (DE, ES, LU, NL, SI, PT and UK). It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LV, LU, NL, SE and SI).

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

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

(d) the data have been unlawfully processed[58];

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[59] [60].

2. (…).

[58] UK scrutiny reservation: this was overly broad.

[59] RO scrutiny reservation.

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

2a. *Where the controller*[61] *(...) has made the personal data public*[62] *and is obliged pursuant to paragraph 1 to erase the data,* the controller, taking account of available technology and the cost of implementation[63], *shall take (...) reasonable steps*[64]*, including technical measures, (...) to inform* **known** *controllers*[65] *which are processing* the *data, that a data subject requests them to erase any links to, or copy or replication of that personal data*[66].

---

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

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

63 Further to NL suggestion. This may hopefully also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;

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

65 BE, supported by ES and FR, suggested referring to 'known' controllers (or third parties).

66 BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule.

3. Paragraphs 1 and 2a shall not apply[67] to the extent that (…) processing of the personal data is necessary:

a. for exercising the right of freedom of expression in accordance with Article 80[68];

b. for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject[69] or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[70];

c. for reasons of public interest in the area of public health in accordance with Article **9(2)(g)(h) and (hb) as well as Article 9(4)**[71];

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

e. (…)

f. (…)

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

---

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

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

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

70 AT scrutiny reservation.

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

4. (…)

5. (…)

Article 17*a*

Right to restriction of processing

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

   (a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[72];

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

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

2. (…)

3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest[73].

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

[73] DE, ES and SI asked who was to define the concept of public interest. DE reservation.

4. A data subject who obtained the restriction of processing pursuant to paragraph 1 (…) shall be informed by the controller before the restriction of processing is lifted[74].

5. (…)

5a. **(…)**[75]

Article 17b

Notification obligation regarding rectification, erasure or restriction[76]

The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient[77] to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

---

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

75 Deleted in view of the new article 83.

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

77 BE, supported by ES and FR, suggested referring to 'known' recipients.

Article 18

Right to data portability[78]

1. (…)

2. **T**he data subject shall have the right to **transmit the personal data**[79] **concerning him or her which he or she has provided to a controller to another controller** in a commonly used[80] **and**[81] **machine-readable** format without hindrance from the controller **to which the data have been provided to**, where
(a) **the processing is based on** consent **pursuant to point (a) of Article 6(1)or point (a) of Article 9 (2)** or on a contract **pursuant to point (b) of Article 6 (1) ; and**

---

78 UK reservation: while it supports the concept of data portability in principle, the UK considers it not within scope of data protection, but in consumer or competition law. Several other delegations (DK, DE, FR, IE, NL, PL and SE) also wondered whether this was not rather a rule of competition law and/or intellectual property law or how it related to these fields of law. Therefore the UK thinks this article should be deleted. NL and CZ thought its scope should be limited to social media. DE, DK and UK pointed to the risks for the competitive positions of companies if they were to be obliged to apply this rule unqualifiedly and referred to/raises serious issues about intellectual property and commercial confidentiality for all controllers. DE, FI, SE and UK also underscored the considerable administrative burdens this article would imply. DE and FR referred to services, such as health services where the exercise of the right to data portability might endanger on-going research or the continuity of the service. Reference was also made to an increased risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects (UK). DE, ES, FR, HU, IE and PL were in principle supportive of this right. SK thought that the article was unenforceable and DE referred to the difficulty/impossibility to apply this right in 'multi-data subject' cases where a single 'copy' would contain data from several data subjects, who might not necessarily agree or even be known or could not be contacted. BE, CZ and RO thought that the exclusion of the public sector should be mentioned not only in recital 55, but also here (ES was opposed thereto).

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

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

81 PT thought 'and' should be deleted.

(b) **the** processing is carried **out by automated means**[82]**.**

2a. The exercise of this right shall be without prejudice to Article 17.

2aa. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights in relation to the processing of the **those personal** data[83].

[3. The Commission may specify (…) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).] [84]

4. (…)[85].

---

82 BE, DE, ES, IE, FI and FR these delegations thought emphasis should be put on the right to withdraw data, also with a view to creating an added value as compared to the right to obtain a copy of personal data. VY and HU also thought the obligation of the controller should be emphasised.

83 ES thought there should be an exception in case disproportionate efforts would be required.

84 FR, HU, SE and UK reservation: this would better set out in the Regulation itself.

85 Deleted in view of the new articles 83a to 83c.

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19

Right to object[86]

1. The data subject shall have the right to object, on reasoned[87] grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point **(…)** (f) of Article 6(1)[88]**;** the personal data shall no longer be processed unless the controller demonstrates (…) legitimate grounds for the processing which override the interests or (…) rights and freedoms of the data subject[89].

---

86 DE, ES, EE, AT, SI, SK and UK scrutiny reservation.

87 COM reservation.

88 The reference to point (e) of Article 6(1) was deleted in view of the objections by BE, CZ, DE, DK, FR and HU. COM reservation on deletion. UK, supported by DE, queried whether the right to object would still apply in a case where different grounds for processing applied simultaneously, some of which are not listed in Article 6. ES and LU queried why Article 6(1) (c) was not listed here.

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

1a. (…) Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)[90] process the personal data concerned except for the establishment, exercise or defence of legal claims[91].

2. Where personal data are processed for direct marketing[92] purposes, the data subject shall have the right to object (…) at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…) and shall be presented clearly and separately from any other information[93].

---

90 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'.

91 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.

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

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

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

3. (...)

4. **(…)**[94]

Article 20

Profiling[95]

1. **The** data subject shall have the right not to be subject to a decision **evaluating personal aspects relating to him or her, which is** based solely **on automated processing, including** profiling**, and** *produces legal effects* concerning him or her or **significantly** [96] affects him or her.

---

94 Deleted in view of the new article 83.

95 DE, ES, FR, AT, PL, SE and UK scrutiny reservation. COM reservation: COM is of the opinion that that the level of data protection in the current draft of this article is below that of Directive 95/46. DE thinks this provision must take account of two aspects, namely, whether and under what conditions a profile (= the linking of data which permits statements to be made about a data subject's personality) may be created and further processed, and, secondly, under what conditions a purely automated measure based on that profile is permissible if the measure is to the particular disadvantage of the data subject. It appears expedient to include two different rules in this regard. According to DE Article 20 only covers the second aspect and DE would like to see a rule included on profiling in regard to procedures for calculating the probability of specific behaviour (cf. Article 28b of the German Federal Data Protection Act, which requires that a scientifically recognized mathematical/statistical procedure be used which is demonstrably essential as regards the probability of the specific behaviour).

96 DE and PL wondered whether automated data processing was the right criterion for selecting high risk data processing operations and provided some examples of automated data processing operation which it did not consider as high risk. DE and ES pointed out that there are also cases of automated data processing which actually were aimed at increasing the level of data protection (e.g. in case of children that are automatically excluded from certain advertising).

1a. **A data subject may be subject to a decision referred to in paragraph 1 only if it**

(a) is **necessary for** entering into, or performance of, a contract between the data subject and a data controller **(…)**[97]; or

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

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

1b. **In cases referred to in paragraph 1a) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision**[98];

2. (…)

3. **Decisions referred to in paragraph 1a** shall not (…) be based on special categories of personal data referred to in Article 9(1), unless **points (a) or (g) of** Article 9(2) **apply** and suitable measures to safeguard the data subject's **rights and freedoms and** legitimate interests [99] are in place.

4. (…)

5. (…)

---

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

98 NL had proposed to use the wording 'and arrangements allowing him to put his point of view, inspired by Article 15 of Directive 95/46.

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

SECTION 5
RESTRICTIONS

Article 21

Restrictions[100]

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in (…) Articles 12 to 20 and Article 32, as well as Article 5[101] in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 20, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

   (aa) national security;

   (ab) defence;

   (a) public security;

   (b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, safeguarding public security[102], or the execution of criminal penalties;

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

---

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

101 AT reservation.

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

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

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

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

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

(g) the enforcement of civil law claims.

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

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS[103]

Article 73

Right to lodge a complaint with a supervisory authority[104]

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single supervisory authority, in particular[105] in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation[106].

2. (…)

3. (…)

4. (…)

5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant **to** Article 74[107] **(…).**

---

103 AT, FR, EE, ES and RO scrutiny reservation.

104 BE, CY, CZ, EE, IE, LY, PT and SI scrutiny reservation.

105 COM, BG, IT and LU though that the data subject should be able to lodge a complaint with any DPA without limitation since the protection of personal data was a fundamental right.

106 DE, supported by NL, suggested adding "when its rights are not being respected".

107 NL and FR scrutiny reservation. Article 54c (2) already provides for a general duty for the supervisory authority with which a complaint has been lodged to notify the data subject of any measures taken (i.e. the scenario of a 'positive' reply by the DPA).

Article 74

Right to an effective judicial remedy against a supervisory authority[108]

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. (...)[109].

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority competent in accordance with Article 51[110] does not deal with a complaint or does not inform the data subject within three months or any shorter period provided under Union or Member State law[111] on the progress or outcome of the complaint lodged under Article 73[112].

3. **Without prejudice to Article 267 TFEU, p**roceedings against a (…) supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established[113].

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or **a** decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

4. (…)

5. (…)[114]

---

108 ES, PT and SI reservation. EE, IT and UK scrutiny reservation.

109 DE, supported by IE and SE, suggested adding: 'by which it is adversely affected'.

110 COM reservation.

111 SI indicated that under its law the DPA was obliged to reply within two months.

112 SE scrutiny reservation. BE reservation. BE said that there was a link to Article 53 and the main establishment and the DPA of the habitual residence. Support from NL. IT thought that paragraphs 1 and 2 overlapped. NO wanted to delete paragraph 2 since a court review would endanger the independency of the DPA.

113 IT suggests stating that proceedings may be brought before the courts of the Member state where the natural or legal person has his/her habitual residence or is established.

114 COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.

Article 75

Right to a judicial remedy against a controller or processor[115]

1. Without prejudice to any available administrative or non-judicial remedy[116], including the right to lodge a complaint with a supervisory authority under Article 73, a data subject shall have the right to an effective judicial remedy[117] if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment (…)[118]. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority acting in the exercise of its public powers.

3. (…)

4. (…)

---

115 DE, EE, PL, PT, SI and SK scrutiny reservation. ES, IT reservation.

116 SI wanted to delete *non-judicial remedy*.

117 ES asked how judicial remedy would be interpreted and how a missed deadline or that there will be no judicial review would be considered.

118 In view of the concerns raised, the reference to national law has been kept only in recital 113.

Article 76 [119]

Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, *which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data,*[120] *to lodge the complaint on his or her behalf*[121] and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf[122].

1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1[123] shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51[124] if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.[125]].

---

119 DE, ES, PT, RO and SI scrutiny reservation. CZ, EE, IT, NL, SI and UK thought this article was superfluous.

120 COM said that consumer organisations and data protection organisations enhance fundamental rights so it was important that they could lodge complaints.

121 IT scrutiny reservation.

122 DE parliamentary reservation; BE, EE reservation and IT scrutiny reservation. EE, supported by FI and SE, thought that the data subject could choose anybody to represent her/him so this drafting was a limitation so a reference to national law was needed. Support from SE.

123 PL asked how an organisation could know about a breach. PT did not want to exclude the possibility of an organisation to lodge complaint if that was provided in national law but meant that the wording was not clear.

124 COM reservation on limitation to competent supervisory authority.

125 This paragraph was moved from Article 73(3). BE, EE, FR reservation. BG, DE, DK, IT, LU, NL, PT and UK scrutiny reservation. UK in particularly queried whether such possibility would also be open to an association when the data subject itself considered that the reply he/she had received was satisfactory. ES on the contrary thought that this possibility should not be limited to data breaches. UK thought that paragraph 1 was sufficient. For DK, PL and SE it was not acceptable that an organisation etc. had an independent right to lodge a complaint.

2. (…)

3. (…)

4. (…)

5. (…)[126]

Article 76a

Suspension of proceedings[127]

1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are pending in a court in another Member State, it shall[128] contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings involving the same processing activities are pending in a court in another Member State, any competent court other than the court first seized may suspend[129] its proceedings.

---

126 COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.

127 AT, BE, DK, EE, ES, FI, FR, IT, NL, PL, PT, SE and SI scrutiny reservation. ES thought that *lis pendens* necessitated the same persons, same proceeding, same object of dispute and same claim and that that could be difficult to establish.UK, supported by FR, cautioned against having a too prescriptive text, support from FR SE thought that GDPR should not regulate *lis pendens*, instead it should be up to the DPA and MS courts to decide. For LU this was a question of judicial cooperation between judicial authorities. NO and FR asked how this text related to Regulation No 44/2001 and the Lugano Convention FI considered that it was necessary to have rules on this question in GDPR.

128 LU supported by EL, suggested to replace "shall" with "may".

129 NL and PL thought that it was difficult to force courts to stay proceedings waiting for another court to decide. NL asked how it was possible for a court to know that another case was going on elsewhere. COM thought that limitation to "same parties" was not appropriate here.

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.[130]

Article 76b

Actions before the Court of Justice of the European Union against decisions by the European Data Protection Board

1. (…)

2. (…)

[130] Based on Article 28 of Brussels I Regulation.

3. **(…)**

4. **(…)**

5. **(…)**

Article 77

Right to compensation and liability[131]

1. Any person who has suffered [132]damage[133] as a result of a processing operation which is not in compliance [134] with this Regulation shall have the right to receive compensation from the controller or processor[135] for the damage suffered.[136]

2. [137]Where more than one controller or processor or a controller and processor are involved in the processing which gives rise to the damage, each controller or processor shall be jointly[138] and severally liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors[139].

---

131 Several Member States (DE, NL and UK) have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. IT suggested specifying that these rules are to be applied according to national law, support from CZ, NL, RO and SI. COM thinks that it has to be left to ECJ to interpret these rules and concepts. FR scrutiny reservation; FR questioned the division of responsibilities and the link to Articles 24 and 25 and national law in this field as well as the principle of subsidiarity.

132 DE, HU and SK suggested adding "material or immaterial/moral". NO suggested clarifying this in a recital.

133 BE asked whether a violation of the principles of the Regulation was enough to constitute a damage or whether the data subject had to prove a specific damage (*obligation de moyens ou de résultat*). COM said that the data subject had to prove the damage.

134 COM reservation as the current draft (contrary to the initial version and the 195 Directive) no longer embodies the principle of strict liability.

135 DE suggested restricting the possibility to seek compensation from the processor to cases where, in violation of point (a) of paragraph 2 of Article 26, the processor has processed personal data contrary to or in the absence of instructions from the controller. ES suggested adding a reference to 'a right to exercise a direction action', but this is already encompassed in the current draft.

136 SE supported by HU considered that Article 77 was unclear and wanted to know whether both an economic and immaterial damage was covered.

137 IE queried why the reference to Article 24(2) had been removed and then the second sentence had been added: what the purpose to bring a claim against all of them and then sort out the individual responsibility?

138 UK thought that one controller or processor might be more responsible than another so it should be allowed for a relative responsibility. SE said that according Directive 95/46 (Article 23) the burden of proof and division of responsibility between the controller and the processor it was only the controller that was held responsible.

139 SI reservation: SI thought this paragraph could be deleted and left entirely to national law.

3. The controller or the processor may[140] be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage[141].

4. Court proceedings for exercising the right to receive compensation shall be brought before the courts with jurisdiction for compensation claims under national law of the Member State referred to in paragraph 2 of Article 75.

Article 78

Penalties

(…)[142]

[140] PL thought this should be turned into a mandatory provision.

[141] DE and PL thought this paragraph needed to be further elaborated. DE in particular thought that the relationship to Article 39 needed to be further clarified. SI thought an arrangement for strict liability in the case of processing by public bodies should be inserted into this paragraph.

[142] This Article was moved to Article 79b. Scrutiny reservation by SK, RO and PT.

Article 79

General conditions for imposing administrative fines[143]

1. Each supervisory authority [competent in accordance with Article 51] shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 53[144].

2. Administrative fines imposed pursuant to Article 79a shall in each individual case be effective, proportionate and dissuasive.

2a. When deciding whether to impose an administrative fine in addition to, or instead of, measures referred to in points (a) to (f) of paragraph 1b of Article 53[145] and [146]deciding on the amount of the administrative fine in each individual case due regard shall be had to the following:

(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned;

(b) the intentional or negligent character of the infringement,

(c) the number of data subjects affected by the infringement and the level of damage suffered by them;

---

143 DK reservation on the introduction of administrative fines in the text as administrative fines – irrespective of their level – raise constitutional concerns. PL thought that Article 79 should set out guidelines only, with possibly a maximum threshold for the DPA to impose fines.

144 Some delegations thought that the corrective measures of Article 53 (1b) should be listed rather here.

145 Moved here from paragraph 2b (further to remarks by FR, IE, IT and CZ).

146 Some delegations (EE, SK, PL) thought that aggravating circumstances should be distinguished from mitigating circumstances. SK suggested laying down exact thresholds (e.g. more than 2/3 of the maximum fine in case of aggravating circumstances). IT thought the possibility of EDPB guidance should be referred to here. NL thought that the status of codes of conduct and certification as well as the consequences of adhering to them needed to be looked at.

(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;

(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;

(f) any previous infringements by the controller or processor;

[(g) any financial benefits gained, or losses avoided, directly or indirectly from the infringement[147];]

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement[148];

(i) **in case** measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, **have previously been** ordered against the controller or processor concerned with regard to the same subject-matter[149], *compliance with **these measures*** ;

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39[150];

---

147 DK, ES and SI reservation. SI stated that a DPA was not equipped to assess this.

148 CZ was concerned that this factor might amount to a violation of the privilege against self-incrimination

149 This should also accommodate concerns regarding the privilege against self-incrimination by removing a general reference to co-operation in the investigation. IT thought this paragraph should refer more generally to previous incidents. DE pleaded for its deletion.

150 DE reservation: DE pointed out that non-adherence to approved codes of conduct or approved certification mechanisms could as such not amount to a violation of the Regulation.

(k) (…)[151];

(l) (…)[152];

(m) any other aggravating or mitigating factor applicable to the circumstances of the case.

2b. (…).

3. (…)[153]

3a. (…)[154]

3b. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State[155].

4. The *exercise by the supervisory authority* [competent in accordance with Article 51] of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.

---

151 Removed at the suggestion of DE and SK.

152 If Member states are entirely free to decide whether or not to provide for sanctions against public authorities, it does not seem appropriate to list the fact that the controller is a public body here.

153 COM reservation on deletion; linked to reservation on Article 79a.

154 COM reservation on deletion.

155 DE would prefer to rule out this possibility in the Regulation. ES thought it should be provided that no administrative fines can be imposed on the public sector.

Article 79a

Administrative fines[156157]

1. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] %[158] of its total worldwide annual turnover[159] of the preceding financial year, on a controller who, intentionally or negligently[160]:

(a) does not respond within the period referred to in Article 12(2) to requests of the data subject;

(b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.

---

156 DK reservation on the introduction of administrative fines in the text as administrative fines – irrespective of their level – raise constitutional concerns. DE, EE, ES, PT and SI scrutiny reservation. FI and SI reservation. COM reservation on replacing 'shall' by 'may' and the deletion of amounts and percentages in paragraphs 1, 2 and 3. DE wanted the risk-based approach to be made clearer. DE thought that proportionality was important because Article 79a concerned fundamental rights/rule of law and deemed it disproportionate that a supervisory authority could impose a fine that the data subject was unaware of. DE said that it was necessary to set out the fines clearly and that the one-stop shop principle did not allow for exceptions being set out in national law. IE thought e gravity of offences was not sufficiently illustrated, *e.g.* infringement in para. 3(m), which according to IE is the most serious one. FR reservation: the strictness of the text may impinge on the independence of the DPA.

157 A majority of Member States (BE, CY DE, EE, ES, FI, IT, LV, LU, MT and NL) appear to be in favour of different scales of sanctions. COM referred to the Market Abuse Regulation with three levels of fines. DK, HU, IE, SE and UK were opposed to maintaining different sanctions scales. FR and PL did not favour it, but could accept it.

158 EE did not consider it appropriate to set out sanctions in percentage because the sanction was not predictable.. PT considered that there should be minimum penalties for a natural person and that for SMEs and micro enterprises the volume of the business should not be looked at when applying the fines (this factor should only be applicable for multinationals). PL thought that administrative fines should be implemented in the same way in all MS. PL said that the fines should be flexible and high enough to represent a deterrent, also for overseas companies.

159 UK commented that *turnover* was used in competition law and asked whether the harm was the same here. EE asked how the annual turnover was connected to the sanction. SI thought that compared to competition law where the damage concerned the society as a whole, data protection concerned private infringements. COM said that both competition law and data protection concern economic values, whereas data protection protects values of the data subject.

160 IT wanted to delete "intentionally or negligently" and thought that those notions were already integrated part of the mechanism to calculate fines.

2. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual (…) turnover of the preceding financial year[161], on a controller or processor who, intentionally or negligently:[162]

(a) does not provide the information, or (…) provides incomplete information, or does not provide the information timely or in a sufficiently transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;

(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19;

(c) (…);

(d) (…);

(e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;

(f) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4).

(g) (…)

[161] DE suggestion.

[162] IT considered that paragraphs 2 and 3 were very generic and only described the infringements but that the scale of gravity was not well defined. IT asked for a better categorisation of the infringements.

3. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year[163], on a controller or processor who, intentionally or negligently:

(a) processes personal data without a (…)[164] legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;

(b) (…);

(c) (…);

(d) does not comply with the conditions in relation to (…) profiling pursuant to Article 20;

(e) does not (…) implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 (…) and 30;

(f) does not designate a representative in violation of Article 25;

(g) processes or instructs the processing of personal data in violation of (…) Articles 26;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;

(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);

(j) (…);

(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

---

163 DE suggestion.

164 FI pointed out that "sufficient" was unclear taking into consideration of the principles in Article 6 (f).

(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).

(n) (…)[165]

(o) (…).

[3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.]

4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.][166]

[165] IT wanted to reinstate failure to cooperate with the DPO. IE that thought that this was a subjective infringement.

[166] CZ, DE, NL and RO reservation. NL that thought that guidelines from the EDPB could solve the problems on the amounts. CZ wanted to delete the paragraph and thought that the DPA could set out the amounts.

Article 79b

Penalties[167]

1. *For infringements of the provisions of this Regulation not listed in Article 79a Member States shall*[168] *lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (...). Such penalties shall be effective, proportionate and dissuasive.*

2. *(...).*

3. *Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.*

---

[167] DE, DK, EE, ES, IT, PL and PT and SK scrutiny reservation. COM explained that infringements not listed in Article 79a were those under national law, referred to in Chapter IX, for example infringements in employment law and relating to freedom of expression. In that way Article 79b is complementary to the list in Article 79and does not exclude other penalties. IT thought it was better to delete the Article but lay down the possibility to legislate at national level. FR reservation on the imposition of criminal penalties. DE in favour of referring *expressis verbis* to criminal penalties.

[168] BE and EE reservation.