



Council of the  
European Union

Brussels, 10 August 2015  
(OR. en)

11428/15

---

---

**Interinstitutional File:  
2012/0010 (COD)**

---

---

**LIMITE**

**DATAPROTECT 131  
JAI 612  
DAPIX 139  
FREMP 171  
COMIX 361  
CODEC 1106**

**NOTE**

---

From:	UK delegation
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. Cion doc.:	5833/12
Subject:	Comments from the UK delegation on Chapters II, III and IV

---

In view of the DAPIX meeting on 3-4 September 2015, delegations will find attached comments from the UK delegation on Chapters II, III and IV of the draft Data Protection Directive.

The UK would like to thank the Presidency for the prompt issuing of the paper on Chapters II, III and IV ahead of the DAPIX meeting on 3-4 September (issued 28 July, 10964/15).

The UK would like to reaffirm our written comments that we have already submitted on these chapters as they were not reflected in document 10964/15 and to present here a summary of our key priorities for these chapters and drafting proposals to reflect them.

Please note that this is without prejudice to any further comments that we may make. In particular, we are likely to have supplementary comments on the additional drafting changes and the questions asked by the Presidency for discussion that are outlined in 10964/15 for the DAPIX meeting on 3-4 September.

## Chapter II

1. **There is no need for Article 7a on specific processing conditions.** Either the Directive or Regulation will apply depending on the purpose of the transfer. We think the text can be simplified if Article 7a is removed. In any event, Article 7a(1), and in particular the following wording: “only if no rights or legitimate interests of the data subject are affected” are operationally unworkable and could undermine police effectiveness and the maintenance of public safety.
2. **It is essential that the processing of sensitive data can take place where strictly necessary for the purposes outlined in Article 1(1) of the Directive.** There is inconsistency in the text with some articles referring directly to purposes set out in Article 1(1), while others do not. That inclusion in some other articles makes it unclear that Article 8 refers to the purposes in Article 1(1). We have suggested drafting to resolve this issue, see Annex A.

## Chapter III

3. **The ability for law enforcement agencies to “Neither Confirm Nor Deny” (NCND) in response to access requests by the data subject is an important operational requirement that needs to be safeguarded.** We welcome that the draft Directive includes provisions which allow for this, but we think that other parts of the text must be clarified to make sure that it is incorporated in all circumstances. This includes the need to ensure that NCND is respected by a supervisory authority in the course of their activities, see Annex B.
4. These provisions must not create unacceptable burdens on law enforcement agencies. **We consider that a law enforcement agency should be able to charge a not excessive amount when providing access for the data subject.** This is currently the case under Article 17 of the current Data Protection Framework Decision (DPFD). We have proposed “without an excessive charge”, wording which is already used in Article 12(2) of the new text, see Annex B.

## Chapter IV

We consider that the **current draft of the text has much more onerous requirements in relation to logging and record keeping than the existing framework.** We want to reduce these burdens by aligning Article 24 of the new text more closely with Article 10 of the DPFD. We have suggested drafting to this effect, see Annex C.

**Annex A – Chapter II: Drafting proposals**

2. It is essential that the processing of sensitive data can take place where strictly necessary for the purposes outlined in Article 1(1) of the Directive.

Article	Drafting proposal	
8	The processing of personal data revealing racial or ethnic origin, political opinions, <u>religious</u> or <u>philosophical</u> beliefs, trade-union membership, <u>and the processing</u> of genetic data or of data concerning health or sex life <u>shall only be allowed when strictly necessary for the purposes set out in Article 1(1) and</u>	A reference to the purposes in Article 1(1) is needed here in order to be consistent with other articles of the Directive which refer to the purposes in Article 1(1) (e.g. Articles 4 and 7). This is to ensure that it is clear that the processing of personal data under Article 8 should be for one or more of the purposes covered by the Directive.

**Annex B – Chapter III: Drafting proposals**

- 3. The ability for law enforcement agencies to “Neither Confirm Nor Deny” (NCND) in response to access requests by the data subject is an important operational requirement that needs to be safeguarded.**

Article	Drafting proposal	Explanation
10 (2)	Member States shall provide that <u>the controller shall take appropriate measures to provide any information referred to in Articles 11 and 11a and any communication under Articles 12 and 15 and 29 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language</u> <b>unless doing so would undermine a purpose of the processing under Article 13(1).</b>	We suggest these additions to make clear that the ability to “neither confirm nor deny” is retained.
10(3)	Member States shall provide that the controller takes all reasonable steps to <u>provide the information referred to in Articles 11 and 11a and to facilitate the exercise of data subject rights under Articles 12 and 15</u> <b>unless doing so would undermine a purpose of the processing under Article 13(1).</b>	

10(4)	<p><u>In cases referred to in Articles 12 and 15, Member States shall provide that the controller informs the data subject in writing of any refusal or restriction of access, or of any refusal of rectification, erasure or restriction, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy, <b>unless doing so would undermine a purpose of the processing under Article 13(1).</b></u></p>	
12(2)	<p><u>Member States shall provide for the right of a data subject to obtain from the controller, on request and without an excessive charge, a copy of the personal data undergoing processing <b>unless doing so would undermine a purpose of the processing under Article 13(1).</b></u></p>	

14(3)	<p>When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question <b>unless doing so would undermine a purpose of the processing under Article 13(1)</b></p>	<p>We have concerns about how this provision relating to supervisory authorities will ensure that the ability to “neither confirm nor deny” is retained for UK law enforcement agencies. It is an important operational requirement that needs to be safeguarded and we need to make sure that the role of the supervisory authority is consistent with this.</p>
15(1)	<p style="text-align: center;"><i>Article 15</i></p> <p style="text-align: center;"><b><i>Right to rectification, <u>erasure and restriction of processing</u></i></b></p> <p><b><u>This article applies in the case of any data subject having accessed personal data concerning him or her processed by the controller in accordance with this Directive.</u></b></p>	<p>We note that the Eurojust General Approach (document no. 6643/15) provides for the possibility to “neither confirm nor deny” in the case of the right to rectification, erasure and restriction of processing. This is on the basis that an individual could make a speculative request for the rectification/erasure of data, even if they are not sure that it exists, and in such a case the controller would be obliged to inform the individual of the outcome.</p>

		In the Eurojust text, the right to rectification, erasure and restriction of processing only applies once the data subject has already been able to access his or her personal data. We suggest that the same approach should be taken here.
--	--	--

**4. We consider that a law enforcement agency should be able to charge a not excessive amount when providing access for the data subject.**

Article	Drafting proposal
10(5)	Member States shall provide that the information <u>provided...</u>  shall be provided (...) <b>free of charge without an excessive charge</b> [...]
12(1)	<u>Subject to Article 13</u> , Member States shall provide for the right of the data subject to obtain from the controller <u>at reasonable intervals and</u> <b>free of charge without an excessive charge</b> confirmation as to whether or not [...]



