



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 24 September 2012**

---

---

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

---

---

**12918/1/12  
REV 1**

**LIMITE**

**DATAPROTECT 97  
JAI 551  
MI 515  
DRS 101  
DAPIX 94  
FREMP 110  
COMIX 460  
CODEC 1978**

**NOTE**

---

from: Presidency

to: Working Group on Information Exchange and Data Protection (DAPIX)

---

No. Cion prop.: 5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7  
COMIX 61 CODEC 219

---

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) - Questionnaire on administrative burdens, delegated/implementing acts and flexibility in data protection rules for the public sector

---

1. At the July JHA Informal Ministerial Meeting in Nicosia, the Presidency invited Ministers to discuss three horizontal issues arising from the draft General Data Protection Regulation, on which delegations had expressed common concerns in the course of technical discussion in the DAPIX Council Working Party. These concerns specifically related to the administrative burden imposed by the draft regulation, to the application of data protection rules in the private and the public sector and the number of delegated and implementing acts that the proposed Regulation foresees.

2. Discussions at the July Informal Ministerial Meeting were conclusive on the need for a structured approach to identify those articles where:

- (a) administrative burden on SMEs could be reduced on the basis of specific, well-defined criteria;
- (b) a degree of flexibility for the application of data protection rules in the public sector could be achieved and,
- (c) provisions for delegated and implementing acts need to be revised on a case-by-case basis and/or more detailed rules should be built in the substantial provisions.

3. Based on these conclusions, the Presidency has taken the initiative to prepare this document, with the aim of further discussing the issues referred to in paragraph 2 above in the framework of Friends of Presidency meeting(s), which will be convened in due course.

4. Delegations are invited to fill in the annexed tables I and II and answer the question in annex III and send their replies to the General Secretariat of the Council ([guy.stessens@consilium.europa.eu](mailto:guy.stessens@consilium.europa.eu)) by 4 October 2012. Delegations are strongly encouraged to reply as briefly as possible, and where relevant, by stating "yes" or "no".

---

**Administrative Burdens**

For the purposes of this exercise, administrative burdens are defined as the costs incurred by enterprises, the non-profit sector, public authorities and citizens in meeting legal obligations to provide information on their action or production, either to public authorities or to private parties. Information is to be construed in a broad sense, i.e. including labelling, reporting, registration, monitoring and assessment needed to provide the information.<sup>1</sup> For example, pursuant to this definition, obligations on data controllers to notify data breaches and to maintain documentation of processing operations would constitute administrative burden, but that would not be the case with obligations to appoint a data protection officer or relating to the right to object, as they do not constitute information obligations, in spite of the fact that they do impose costs of compliance on data controllers. Compliance costs should be distinguished from administrative burdens as they constitute the totality of costs that flow from compliance with a given legal instrument.

In the first column the Commission will provide a list of the provisions that it considers to impose administrative burdens on data controllers. Delegations are free to add additional rows to this table, indicating where appropriate additional provisions of the draft Regulation that they consider to impose administrative burden on controllers. The second column requires delegations to present a brief proportionality assessment of the administrative burden described in the first column. Particular emphasis in this respect should be given to the burden imposed on micro, small and medium-sized enterprises.

---

<sup>1</sup> Definition from European Commission Impact Assessment Guidelines (2009) - [http://ec.europa.eu/governance/impact/commission\\_guidelines/docs/ia\\_guidelines\\_annexes\\_en.pdf](http://ec.europa.eu/governance/impact/commission_guidelines/docs/ia_guidelines_annexes_en.pdf)

The third and fourth columns require an assessment of the appropriateness of the criteria proposed in the draft Regulation by the Commission to promote a risk-based approach and differentiate, in specific cases, the applicability of obligations on data controllers (for example, depending on the nature of the data or the type of processing, nature of the activities of the controller, risks for the data subjects). The last four columns concern additional possible criteria suggested during the technical and political discussions by delegations. In those cases that delegations find that the criteria for the applicability of the listed obligations proposed by the Commission need to be changed, they are requested to indicate which of the other possible criteria in the last four columns they consider to be appropriate for that purpose.

At the end of the table delegations are invited to introduce their commentary on the additional compliance costs imposed by the draft Regulation.

ARTICLE OF DRAFT DP REGULATION	PROPORTIONALITY PRINCIPLE		CRITERIA PROPOSED IN DRAFT DP REGULATION (not mutually exclusive)		OTHER/ADDITIONAL POSSIBLE CRITERIA (not mutually exclusive)			
	Proportionality Test – is the obligation proportional, particularly in terms of the burden it imposes on micro, small, and medium-sized enterprises as compared to large enterprises? (YES/NO)		Is the size of the entity processing the personal data an appropriate criterion for the application of data protection rules in this case? (YES/NO)	Risk involved in the processing activities (e.g. sensitivity of data, systematic monitoring of data subjects) (YES/NO)	Volume of personal data processed (YES/NO)	Number of data subjects affected (YES/NO)	Which category of data subjects is affected (e.g. minors) (YES/NO)	Other (please specify)
<b>Article 11</b> <b>Transparent information and communication</b>  1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication								

<p>relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.</p>								
<p><b>Article 12 Procedures and mechanisms for exercising the rights of the data subject</b></p> <p>1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.</p>								

<p>Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.</p> <p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be</p>								
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p><b>3.</b> If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> <p><b>4.</b> The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge</p>								
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.<sup>2</sup></p>								
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

---

\* [...] indicates that a certain part of the text has been omitted, namely provisions concerning delegated and implementing acts as these are dealt with in separate tables.

<p><b>Article 14</b> <b>Information to the data subject</b></p> <p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p><b>(a)</b> the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p><b>(b)</b> the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p>								
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by</p>								
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>the Commission;  <b>(h)</b> any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p><b>2.</b> Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p><b>3.</b> Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the</p>								
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>personal data originate.</p> <p><b>4.</b> The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p><b>(a)</b> at the time when the personal data are obtained from the data subject; or</p> <p><b>(b)</b> where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> <p><b>5.</b> Paragraphs 1 to 4 shall not apply, where:</p> <p><b>(a)</b> the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p><b>(b)</b> the data are not</p>								
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort;</p> <p>or</p> <p><b>(c)</b> the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p><b>(d)</b> the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.</p> <p><b>6.</b> In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p>										
<b>Article 15</b>										

<p><b>Right of access for the data subject</b></p> <p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p>								
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>(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;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the</p>								
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.								
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p><b>Article 22</b> <b>Responsibility of the controller<sup>3</sup></b></p> <p><b>1.</b> The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p><b>2.</b> The measures provided for in paragraph 1 shall in particular include:</p> <p><b>(a)</b> keeping the documentation pursuant to Article 28;</p> <p><b>(b)</b> implementing the data security requirements laid down in Article 30;</p> <p><b>(c)</b> performing a data protection impact assessment pursuant to Article 33;</p>								
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<sup>3</sup> Article 22 covers also the evidence and documentation the controller shall provide to ensure compliance with other relevant provisions of this Chapter, as referred to in the Article.

<p>(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);</p> <p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p>								
<p><b>Article 28</b></p> <p><b>Documentation</b></p> <p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations</p>								

<p>under its responsibility.</p> <p><b>2.</b> The documentation shall contain at least the following information:</p> <p><b>(a)</b> the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p><b>(b)</b> the name and contact details of the data protection officer, if any;</p> <p><b>(c)</b> the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p><b>(d)</b> a description of categories of data subjects and of the categories of personal data relating to them;</p> <p><b>(e)</b> the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the</p>								
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>legitimate interest pursued by them;  <b>(f)</b> where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;  <b>(g)</b> a general indication of the time limits for erasure of the different categories of data;  <b>(h)</b> the description of the mechanisms referred to in Article 22(3).  <b>3.</b> The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p>								
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p><b>(a)</b> a natural person processing personal data without a commercial interest; or</p> <p><b>(b)</b> an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p>								
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p><b>Article 31</b>  <b>Notification of a personal data breach to the supervisory authority</b></p> <p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 must at least:</p>								
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p> <p>(c) recommend measures to mitigate the possible adverse effects of the personal data breach;</p> <p>(d) describe the consequences of the personal data breach;</p> <p>(e) describe the measures proposed or taken by the controller to address the personal data breach.</p> <p>4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken.</p>								
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

--	--	--	--	--	--	--	--	--

<p><b>Article 32</b>  <b>Communication of a personal data breach to the data subject</b></p> <p>1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p> <p>2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).</p> <p>3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates</p>								
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--

<p>to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p>								
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--	--	--



**Delegated Acts in the proposed General Data Protection Regulation**

1. The Presidency finds it useful to reproduce below a general explanation on delegated acts as transmitted by the Commission:

*According to the Treaty of the Functioning of the European Union, when the Commission receives the power to adopt delegated acts under Article 290 the Commission is authorised to supplement or amend certain non-essential elements of the legislative act. Such a delegation is always discretionary: the legislator delegates its powers to the Commission in the interests of efficiency (cf. COM (2009) 673 final). The Commission, when preparing and drawing up delegated acts, will carry out appropriate and transparent consultations well in advance, including at expert level (“Common Understanding on delegated acts”, II.4, [Council doc 8753/11]). The delegation of power may be revoked at any time by the European Parliament or by the Council and the delegated act only enters into force if neither Parliament nor Council object (see Article 86 of the proposed Regulation). The use of delegated powers will depend on technological, economic and social developments, as well as on the experience with the practical application of the Regulation.*

2. In addition, the Presidency finds its useful to draw the attention of delegations to the recent judgment of 5 September 2012 of the EU Court of Justice about the notion of essential and non-essential elements when conferring delegated or implementing powers (Case C-355/10) in which the Court said that "*ascertaining which elements of a matter must be categorised as essential is not (...) for the assessment of the [EU] legislature alone, but must be based on objective factors amenable to judicial review*" (point 67), that account should be taken "*(...) of the characteristics and particularities of the domain concerned*" (point 68) and that "*provisions on conferring powers of public authority [such as in the case at stake which concerned enforcement powers of border guards] mean that the fundamental rights of the persons concerned may be interfered with to such an extent that the involvement of the [EU] legislature is required*" (point 77).

**Delegated Acts in the proposed General Data Protection Regulation**

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
<p><b>6. Lawfulness of processing</b>  <b>6.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a <u>child</u>.</u></p>	<p>Point (f) of Article 6(1) deals with the “balance of interests” as a legitimate ground for processing. The provision, already present in Directive 1995/46/EC (Article 7(f)), is further specified in the proposal (e.g.: when the data subject is a child; non application of this ground to processing carried out by public authorities in the performance of their tasks).<sup>6</sup> Should the need for further clarification arise also in light of technological developments, there is the possibility to supplement the “balance of interests” clause of Article 6(1)(f) by further</p>		

<sup>4</sup> According to Article 86(2) of the proposal the "delegation of power conferred on the Commission in [*the relevant Articles of the Regulation*] shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of the Delegation."

<sup>5</sup> Options to replace the suggested provision with:  
<sup>1</sup> More detailed rules in the substantive provisions;  
<sup>2</sup> Codes of conduct;  
<sup>3</sup> Other (please specify).

<sup>6</sup> See also provisions on information and documentation (Article 14, Article 28) as regards Article 6(1)(f).

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
	specifying the conditions for particular cases/contexts.		
<p><b>8. Processing of personal data of a child</b></p> <p><b>8.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the methods to obtain verifiable consent</u> referred to in paragraph 1. In doing so, the Commission shall consider specific measures for <u>micro, small and medium-sized enterprises</u>.</p>	<p>Article 8 specifies the conditions for consent for children below the age of 13 years in relation to the offering of information society services directly to a child.</p> <p>Possibility to supplement Article 8 with further specifications e.g. for practical arrangements for verifiable consent by child's parents, taking into account technological developments (e.g. communication by fax, e-mail, new mobile applications).</p>		
<p><b>9. Processing of special categories of personal data</b></p> <p><b>9.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria, conditions and appropriate safeguards</u> for the processing of the special categories of personal data <u>referred to in</u></p>	<p>This Delegated Act <u>cannot extend the list of sensitive data</u> provided for by Article 9(1)).</p> <p>The situations (exhaustive list) where processing of special categories of data is allowed are foreseen in Article 9(2).</p> <p>Possibility to supplement Article 9 in order to, for example:</p>		

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
<u>paragraph 1 and the exemptions laid down in paragraph 2.</u>	<ul style="list-style-type: none"> <li>- provide safeguards in view of technological developments, e.g. for the processing of sensitive data in the context of health information for flights;</li> <li>- clarify which situations could be covered, and which are not, by “manifestly made public” in Article 9(2)(e);</li> <li>- further clarify when processing is necessary “for the establishment of legal claims” under Article 9(2)(f).</li> </ul>		
<p><b>12. Procedures and mechanisms for exercising the rights of the data subject</b></p> <p><b>12.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and conditions</u> for the <u>manifestly excessive requests</u> and the <u>fees</u> referred to in paragraph 4.</p>	<p>The principle of "free of charge access" and the possibility to impose a fee in case of manifestly excessive requests are set in Article 12(4). Supplementing Article 12 might be necessary for example:</p> <ul style="list-style-type: none"> <li>- for further specifying what constitutes a “manifestly excessive” access request by a data subject, e.g. by a certain number of requests in a certain period, and</li> <li>- for providing minimum and</li> </ul>		

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
	maximum fees which controllers receiving such "manifestly excessive requests" from a data subject may charge for providing the information or taking the action requested.		
<p><b>14. Information to the data subject</b>  <b>14.7</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1</u>, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the <u>criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations</u>, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5.</p>	<p>The elements as regards the information that must be provided to the data subject are enshrined in Article 14(1) points (a)-(h).</p> <p>Supplementing Article 14 might be necessary in particular in view of technological developments for example to:</p> <ul style="list-style-type: none"> <li>- further define the details for specifying "categories of recipients";</li> <li>- specify the level of information to data subjects as regards transfers of data to recipients in third countries;</li> <li>- specify the situations where specific information on the right to object is necessary, e.g. in the marketing sector.</li> </ul>		

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.			
<p><b>15. Right of access for the data subject</b></p> <p><b>15.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the <u>criteria and requirements for the communication</u> to the data subject of the <u>content of the personal data</u> referred to in point (g) of paragraph 1.</p>	<p>Article 15 provides the elements (information included under points (a) to (h)) to be provided to the data subject in case of an access request.</p> <p>Supplementing Article 15 might be necessary in particular to further clarify the criteria and requirements to easily communicate personal data to the data subject in an online environment, e.g. by online-forms, specific software and secure interface, taking into account technological developments.</p>		
<p><b>17. Right to be forgotten</b></p> <p><b>17.9</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further</p>	<p>The conditions for application of the right to be forgotten are provided for in Article 17(1) – (3).</p>		

Article	Considerations on the proposed DA: objectives, content, scope, likely duration of delegation <sup>4</sup>	Political assessment: is the delegation necessary? (YES/NO)	If not, which alternative solution would you accept? a) Retain the provision, but with stricter conditions on C b) Replace with: <sup>5</sup> c) Delete the provision
<p>specifying: (a) <u>the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations</u>;</p> <p>(b) <u>the conditions for deleting links, copies or replications of personal data from publicly available communication services</u> as referred to in paragraph 2;</p> <p>(c) <u>the criteria and conditions for restricting the processing of personal data</u> referred to in paragraph 4.</p>	<p>Supplementing Article 17 might be necessary for example to clarify:</p> <ul style="list-style-type: none"> <li>- technical conditions for ensuring the erasure of personal data, e.g. rules for deleting http links, meta data and cached data, dead links and other links, copies or replications of personal data, taking into account technological developments.</li> </ul>		
<p><b>20. Measures based on profiling</b></p> <p><b>20.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests</u> referred to in paragraph 2.</p>	<p>Article 20 regulates what constitutes "profiling", as well as the conditions under which a person may be subjected to a measure based on profiling.</p> <p>Article 20(5) provides for the possibility to further specify in particular cases/contexts how to safeguard the data subject's legitimate interests in view of emerging new technologies allowing individual profiling.</p>		

<p><b>22. Responsibility of the controller</b>  <b>22.4</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>specifying any further criteria and requirements for appropriate measures</u> referred to in paragraph 1 other than those already referred to in paragraph 2, <u>the conditions for the verification and auditing mechanisms</u> referred to in paragraph 3 and as regards the criteria for <u>proportionality</u> under paragraph 3, and considering <u>specific measures for micro, small and medium-sized-enterprises</u>.</p>	<p>Article 22 describes the obligations of the controller as regards the demonstration of the compliance with the Regulation.</p> <p>Supplementing Article 22 might be necessary for example to:</p> <ul style="list-style-type: none"> <li>- provide further clarification to controllers on what could be “appropriate measures” in different circumstances (e.g. criteria/minimum requirements for privacy programs in large companies);</li> <li>- provide criteria for audit controls in large companies, taking into account technological developments.</li> </ul>		
<p><b>23. Data protection by design and by default</b>  <b>23.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>specifying any further criteria and requirements for appropriate measures and mechanisms</u> referred to in paragraph 1 and 2, in particular for <u>data protection by design requirements</u></p>	<p>The obligations of the data controllers as regards data protection by design and default are set out in Article 23(1) and (2).</p> <p>Supplementing Article 23 might be necessary to specify the requirements for appropriate data protection by design and data protection by default measures and mechanisms for specific</p>		

<p><u>applicable across sectors, products and services.</u></p>	<p>sectors and/or specific processing operations, in particular in view of technological developments, for example specify minimum requirements for compliance for electrical appliances (cf. Commission recommendation 2012/148/EU on preparations for the roll-out of smart metering systems) or for Radio-frequency identification (RFID) (cf. Commission recommendation C(2009) 3200 final).</p>		
<p><b>26. Processor</b>  <b>26.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</u></p>	<p>The specific obligations and criteria regarding the choice of a processor by a controller, the contract or other legal act governing the relationship between the controller and the processor, are provided for in Article 26.</p> <p>Supplementing Article 26 might be necessary, for example, to further clarify:</p> <ul style="list-style-type: none"> <li>- processor's duties when outsourcing IT services (service, infrastructure or software),</li> <li>- the conditions under which data protection compliance can be ensured when facilitating the processing activities within a group of undertakings and how</li> </ul>		

	control would be secured in relation to such facilitations, taking into account technological developments.		
<p><b>28. Documentation</b></p> <p><b>28.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the documentation</u> referred to in paragraph 1, to take account of in particular the <u>responsibilities</u> of the controller and the processor and, if any, the controller's representative.</p>	<p>The obligations regarding documentation are listed in Article 28.</p> <p>Supplementing Article 28 might be necessary for example to further tailor and clarify the regular requirements for controllers/processors/controller's representatives as regards documentation, taking into account technological developments.</p>		
<p><b>30. Security of processing</b></p> <p><b>30.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the <u>criteria and conditions for the technical and organisational measures</u> referred to in paragraphs 1 and 2, including the determinations of <u>what constitutes the state of the art, for specific sectors and in specific data processing situations</u>, in particular taking account of developments in</p>	<p>The obligations regarding security of processing, including the fact of having a risk based approach, are listed in Article 30.</p> <p>Supplementing Article 30 might be necessary for example to provide conditions for encryption requirements when transmitting sensitive data in the health sector, taking into account technological developments.</p>		

<p>technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p>			
<p><b>31. Notification of a personal data breach to the supervisory authority</b>  <b>31.5</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for establishing the data breach</u> referred to in paragraphs 1 and 2 and for the <u>particular circumstances</u> in which a controller and a processor is required to notify the personal data breach.</p>	<p>The requirements regarding the notification of a breach to the supervisory authority are listed in Article 31.</p> <p>To further specify criteria and conditions for establishing the data breach and with a view to ensuring consistency with the e-privacy Directive 2002/58/EC and its subsequent implementation, this empowerment follows the approach of Article 4(5) of the e-privacy Directive, in order to, in particular:</p> <ul style="list-style-type: none"> <li>- provide criteria to assess the severity of a breach;</li> <li>- define/clarify in which situations the controller is to be held to be “aware” of the breach, taking into account technological developments.</li> </ul>		
<p><b>32. Communication of a personal data breach to the data subject</b>  <b>32.5</b> The Commission shall be empowered to adopt delegated</p>	<p>The requirements regarding the notification of a breach to the data subject are listed in Article 32 (risk based approach).</p>		

<p>acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements</u> as to the <u>circumstances</u> in which a personal data breach is <u>likely to adversely affect</u> the personal data referred to in paragraph 1.</p>	<p>To further specify the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect an individual's personal data and with a view to ensuring consistency with the e-privacy Directive 2002/58/EC, this empowerment follows the approach of Article 4(5) of the e-privacy Directive, in order to, in particular:</p> <ul style="list-style-type: none"> <li>- outline relevant categories of breaches in relation to their adverse effects, e.g. the kind of breach, and whether or not the data was actively used by an intruder;</li> <li>- establish a 'de minimis list' of breaches which would not be considered likely to adversely affect the protection of the personal data or the privacy of the data subject, taking into account technological developments.</li> </ul>		
<p><b>33. Data protection impact assessment</b>  <b>33.6</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and conditions</u> for the processing</p>	<p>The situations where data protection impact assessments have to be carried out are described in Article 33 (risk based approach).</p> <p>As risks to personal data evolve with time, supplementing Article</p>		

<p><u>operations likely to present specific risks</u> referred to in paragraphs 1 and 2 and the <u>requirements for the assessment</u> referred to in paragraph 3, including <u>conditions for scalability, verification and auditability</u>. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>	<p>33 might be necessary in particular to further clarify the criteria for processing operations “likely to present specific risks” and to further clarify, for example, the typical steps for conducting a DPIA (compare with Point I.4 Commission recommendation 2012/148/EU on preparations for the roll-out of smart metering systems), taking into account technological developments.</p>		
<p><b>34. Prior authorisation and prior consultation</b>  <b>34.8</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements</u> for determining the <u>high degree of specific risk</u> referred to in point (a) of paragraph 2.</p>	<p>The principles and conditions for prior authorisation and consultation are listed in Article 34.</p> <p>Supplementing Article 34 might be necessary for example to:</p> <ul style="list-style-type: none"> <li>- further clarify what a risky processing activity is, also in view of technological developments, by identifying specific criteria, i.e. referring to the category of processed data, the degree of risk the processing itself presents in terms of data security, as well as the purpose of processing.</li> </ul>		
<p><b>35. Designation of the data protection officer</b>  <b>35.11</b> The Commission shall be</p>	<p>The requirements and conditions governing DPOs are set out in Article 35.</p>		

<p>empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the core activities of the controller or the processor</u> referred to in point (c) of paragraph 1 and the <u>criteria for the professional qualities of the data protection officer</u> referred to in paragraph 5.</p>	<p>Supplementing Article 35 might be necessary for example to:</p> <ul style="list-style-type: none"> <li>- specify further what constitutes ‘core activities’ of a controller or processor (risk based approach) requiring the designation of a DPO, in particular in the context of technological developments.</li> </ul>		
<p><b>37. Tasks of the Data protection officer</b>  <b>37.2</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for tasks, certification, status, powers and resources</u> of the data protection officer referred to in paragraph 1.</p>	<p>The tasks of the DPO are listed in Article 37.</p> <p>Supplementing Article 37 might be necessary for example to specify further the professional qualities of the data protection officers to avoid fragmentation in the Internal Market.</p>		
<p><b>39. Certification</b>  <b>39.2</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the data protection certification mechanisms</u> referred to in paragraph 1, including</p>	<p>Article 39 introduces the possibility to establish certification mechanisms and data protection seals and marks.</p> <p>Supplementing Article 39 might be necessary for example to define specific requirements regarding the monitoring and renewal of certification standards,</p>		

<p><u>conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.</u></p>	<p>taking into account technological developments.</p>		
<p><b>43. Transfers by way of binding corporate rules</b>  <b>43.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for binding corporate rules</u> within the meaning of this Article, in particular as regards <u>the criteria for their approval</u>, the application of points (b), (d), (e) and (f) of paragraph 2 to <u>binding corporate rules adhered to by processors and on further necessary requirements</u> to ensure the protection of personal data of the data subjects concerned.</p>	<p>Requirements regarding binding corporate rules are listed in Article 43.</p> <p>Supplementing Article 43 might be necessary to ensure uniform interpretation of the criteria and requirements used to declare binding corporate rules valid, for example further specifying the criteria and the evaluation procedures of BCRs for processors (e.g. duration, minimum documentation requirements).</p>		
<p><b>44. Derogations</b>  <b>44.7</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying 'important grounds of public interest'</u> within the meaning of point (d) of paragraph 1 as well as the</p>	<p>The derogations for a data transfer to a third country are listed in Article 44.</p> <p>Supplementing Article 44 might be necessary for example to:</p> <ul style="list-style-type: none"> <li>- publish a list of examples of recognised public interests with references to the underlying EU</li> </ul>		

<p><u>criteria and requirements for appropriate safeguards</u> referred to in point (h) of paragraph 1.</p>	<p>legislation; - provide further clarity on whether and when the involvement of a national data protection authority could constitute an “appropriate safeguard” to allow the transfer.</p>		
<p><b>79. Administrative sanctions</b> <b>79.7</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>updating the amounts of the administrative fines</u> referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	<p>The conditions and maximum amounts for fines are defined in Article 79.</p> <p>Supplementing Article 79 might be necessary to adjust the absolute amounts of the fines in line with inflation.</p>		
<p><b>81. Processing of personal data concerning health</b> <b>81.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying <u>other reasons of public interest in the area of public health</u> as referred to in point (b) of paragraph 1, as well as <u>criteria and requirements for the safeguards</u> for the processing of personal data for the purposes referred to in paragraph 1.</p>	<p>The specific conditions for processing personal data concerning health are listed in Article 81.</p> <p>This empowerment is <u>limited</u> to adding items to the list of examples given in point (b) of Article 81(1), and can only be used to specify the reasons of public interest in the area of public health, such as for the surveillance of wide-spread serious diseases.</p> <p>The Commission may also</p>		

	specify related safeguards, such as appropriate security measures and access rights, taking into account technological developments.		
<p><b>82. Processing in the employment context</b></p> <p><b>82.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.</u></p>	Supplementing Article 82 might be necessary for example to specify requirements for safeguards in the context of IT systems for human resource management, taking into account technological developments.		
<p><b>83. Processing for historical, statistical and scientific research purposes</b></p> <p><b>83.3</b> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of <u>further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.</u></p>	<p>The specific conditions for processing personal data for historical, statistical and scientific purposes are listed in Article 83.</p> <p>Supplementing Article 83 might be necessary for example to clarify the application of pseudonymisation (key-coding) and anonymisation of personal data in specific medical research cases, taking into account technological developments.</p>		

## Implementing Acts in the proposed General Data Protection Regulation

1. The Presidency finds it useful to reproduce below a general explanation on implementing acts as transmitted by the Commission:

*Under Article 291 of the Treaty on the Functioning of the European Union, Member States are primarily responsible for the implementation of Union law but where uniform conditions for implementing legally binding acts are needed, those acts must confer implementing powers on the Commission. The rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers have been laid down in the new "Comitology Regulation (EU) 182/2011", adopted by EP and Council (OJ L 55, 28.2.2011, page 13).*

*To note also that the Data Protection Board, under Article 66 (1) (b), may issue "guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage a consistent application". In practice, if the need for clarification arises, actions of the Data Protection Board, or other measures, such as codes of conduct, may make unnecessary the use of implementing powers. Measures by the Commission in the form of exercise of implementing powers provide an opportunity for the Member States to remain involved in the concretisation of the content of the Regulation with a view to uniform application.*

*As to the implementing powers, they also respond to the legitimate request in particular from controllers for legal certainty. The Commission's implementing measures offer inter alia models and examples which – when used by controllers – facilitate and support compliance with the requirements of the Regulation, and thereby provide legal certainty.*

2. In addition, the Presidency finds its useful to draw the attention of delegations to the recent judgment of 5 September 2012 of the EU Court of Justice about the notion of essential and non-essential elements when conferring delegated or implementing powers (Case C-355/10, quoted above on page 29).

**Implementing Acts in the proposed General Data Protection Regulation**

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>8. Processing of personal data of a child</b>  <b>8.4</b> The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u>                      - provide for a EU model form which can be used to obtain parental consent online</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>12. Procedures and mechanisms for exercising the rights of the data subject</b></p> <p><b>12.6</b> The Commission may lay down <u>standard forms</u> and specifying <u>standard procedures for the communication</u> referred to in paragraph 2, including the <u>electronic format</u>.</p> <p>In doing so, the Commission shall take the <u>appropriate measures for micro, small and medium-sized enterprises</u>. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u></p> <ul style="list-style-type: none"> <li>- specify a standard EU format which can be used for access requests</li> <li>- specify a commonly used electronic format (like plain text, html, pdf, etc.) in order to reduce cost and provide for interoperability, in view of technological developments.</li> </ul>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>14. Information to the data subject</b>  <b>14.8</b> The Commission may lay down <u>standard forms</u> for providing the <u>information</u> referred to in paragraphs 1 to 3, taking into account the <u>specific characteristics and needs of various sectors and data processing situations</u> where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s)</u>:</p> <ul style="list-style-type: none"> <li>- EU standard model forms for providing the information to the data subjects online (compare with the ‘model instructions on withdrawal’ set out in Annex I(A) of Directive 2011/83/EU of 25 October 2011 on consumer rights).</li> <li>- EU standard forms in the context of airline ticket booking</li> </ul>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>15. Right of access for the data subject</b>  <b>15.4</b> The Commission may specify <u>standard forms and procedures for requesting and granting access</u> to the information referred to in paragraph 1, including for <u>verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations</u>. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u></p> <p>- specify how controllers may use official identification documents for verification of the data subject's identity, in the light of technological developments.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>18. Right to data portability</b>  <b>18.3</b> The Commission may specify the <u>electronic format</u> referred to in paragraph 1 and the <u>technical standards, modalities and procedures for the transmission of personal data</u> pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u>  - specify an electronic format which can be used as default standard.</p>		
<p><b>23. Data protection by design and by default</b>  <b>23.4</b> The Commission may lay down <u>technical standards</u> for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u>  - define a technical standard, taking into account the work of technical standardization bodies, in the light of technological developments.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>28. Documentation</b>  <b>28.6</b> The Commission may lay down <u>standard forms for the documentation</u> referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u>  - define for a standard model which can be used in relation to the documentation of human resource management systems.</p>		
<p><b>30. Security of processing</b>  <b>30.4</b> The Commission may adopt, where necessary, implementing acts for <u>specifying the requirements laid down in paragraphs 1 and 2 to various situations</u>, in particular to:  (a) prevent any unauthorised access to personal data;  (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data,  (c) ensure the verification of the lawfulness of processing operations.</p>	<p>This implementing power might be necessary to give effect to Article 30 in a uniform way by way of regulating how the requirements set according to Article 30(3) can be fulfilled.  <u>Example(s):</u>  - define standards for specific processing operations, taking into account work of technical standardization bodies, in the light of technological developments.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>31. Notification of a personal data breach to the supervisory authority</b>  <b>31.6</b> The Commission may lay down the <u>standard format</u> of such notification to the supervisory authority, the <u>procedures</u> applicable to the notification requirement and the <u>form and the modalities for the documentation</u> referred to in paragraph 4, including the <u>time limits for erasure</u> of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Ensuring consistency with the e-privacy Directive 2002/58/EC, this empowerment follows the approach of Article 4(5) of the e-privacy Directive.</p> <p><u>Example(s):</u></p> <p>- define a form/template to be filled in, and clarify for how long it has to be kept.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>32. Communication of a personal data breach to the data subject</b>  <b>32.6</b> The Commission may lay down <u>the format of the communication</u> to the data subject referred to in paragraph 1 and the <u>procedures</u> applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Ensuring consistency with the e-privacy Directive 2002/58/EC, this empowerment follows the approach of Article 4(5) of the e-privacy Directive.  <u>Example(s):</u>  - define a standard online form to be filled in by the controller.</p>		
<p><b>33. Data protection impact assessment</b>  <b>33.7</b> The Commission may specify <u>standards and procedures for carrying out and verifying and auditing the assessment</u> referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Implementing acts might be necessary to give effect to Article 33 in order to facilitate and streamline the preparation of data protection impact assessments.  <u>Example(s):</u>  - define templates developed at Union level.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>34. Prior authorisation and prior consultation</b>  <b>34.9</b> The Commission may set out <u>standard forms and procedures for prior authorisations and consultations</u> referred to in paragraphs 1 and 2, and <u>standard forms and procedures for informing the supervisory authorities</u> pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s):</u>  - establish a standard form which can be used for the electronic transmission and acknowledgement of receipt of data protection impact assessments to Data protection authorities.</p>		
<p><b>38. Codes of conduct</b>  <b>38.4</b> The Commission may adopt implementing acts for <u>deciding that the codes of conduct and amendments or extensions to existing codes of conduct</u> submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p>This might be used to give general validity to codes of conducts within the EU.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>39. Certification</b>  <b>39.3</b> The Commission may lay down <u>technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks.</u>  Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p>This might be used to support and promote technical standards, taking into account the work carried out by EU technical standardisation bodies, and to ensure that data subjects are informed about those standards and consider them when disclosing their personal data.</p>		
<p><b>41. Transfers with an adequacy decision</b>  <b>41.3</b> The Commission may decide that a <u>third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2.</u> Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).  <b>41.4</b> The implementing act shall</p>	<p>Essentially in line with the current adequacy procedures in the context of the current Data protection Directive (see for example Decision 2012/484/EU: Commission Implementing Decision of 21 August 2012 on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal (OJ L 227 , 23/08/2012, p.11))  The proposal creates some flexibility as it would allow for sectoral and/or geographical adequacy.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p>specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.</p> <p><b>41.5</b> The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation <u>does not ensure an adequate level of protection</u> within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in</p>			

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).			
<p><b>43. Transfers by way of binding corporate rules</b></p> <p><b>43.4</b> The Commission may specify the <u>format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities</u> for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p><u>Example(s):</u></p> <p>- define formats and procedures for an online workflow for the fast validation of binding corporate rules.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p><b>55. Mutual assistance</b>  <b>55.10</b> The Commission may specify the <u>format and procedures for mutual assistance</u> referred to in this article and the arrangements for the exchange of information by <u>electronic means</u> between <u>supervisory authorities</u>, and between <u>supervisory authorities and the European Data Protection Board</u>, in particular the <u>standardised format</u> referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><u>Example(s)</u>:  - define formats and procedure for an online secure workflow for the fast exchange of relevant information between data protection authorities for the purpose of mutual assistance.</p>		
<p><b>62. Implementing acts</b>  <b>62.1</b> The Commission may adopt implementing acts for:  (a) <u>deciding on the correct application of this Regulation</u> in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has</p>	<p>Implementing acts might be necessary, as a last resort measure, to give effect to the consistency mechanism and Article 62 in a uniform way by way of :  - deciding on the correct application of this Regulation in the specific cases, on specific matters, in line with the obligation of the Commission to ensure a correct, consistent and effective application of EU law;</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p>been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;</p> <p>(b) deciding, within the period referred to in Article 59(1), whether it declares <u>draft standard data protection clauses</u> referred to in point (d) of Article 58(2), <u>as having general validity</u>;</p> <p>(c) specifying <u>the format and procedures for the application of the consistency mechanism</u> referred to in this section;</p> <p>(d) specifying the arrangements for the <u>exchange of information by electronic means between supervisory authorities</u>, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in</p>	<p>- decide on the general validity for the EU of draft standard data protection clauses;</p> <p>- providing the format and procedures for swift information exchange.</p> <p>Article 62.2 is a safeguard clause to give guidance in situations in which otherwise data subjects would be left without protection due to a possibly inconsistent, ineffective or incorrect application of the Regulation.</p>		

Article	Consideration for proposed IA	Political assessment: is this empowerment necessary? (YES/NO)	If not, which alternative solution would you propose? a) Retain the provision, but with stricter conditions on COM b) Delete the provision c) Other (please specify)
<p>Article 58(5), (6) and (8). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> <p><b>62.2</b> On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.</p>			

**Flexibility in data protection rules for the public sector**

Please list the policy areas, as well as the specific articles in the draft Data Protection Regulation in which, in your opinion, a further degree of flexibility should be granted for the public sector within the Regulation.

1. ...
2. ...
3. ...
4. ...
5. ...

---