COUNCIL OF THE EUROPEAN UNION

Brussels, 31 January 2014

5880/1/14 REV 1

LIMITE

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 14
JAI 47
MI 92
DRS 15
DAPIX 8
FREMP 13
COMIX 69
CODEC 231

NOTE

from:	Presidency
to:	Working Group on Information Exchange and Data Protection (DAPIX)
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) - Data Protection Impact and Prior Checks

Delegations find attached the Presidency proposals regarding data protection impact assessment and prior authorisation.

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes (…). In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the severity and likelihood of these specific risks, taking into account the nature, scope and purposes of the processing and the sources of the risks, which should include in particular the envisaged measures, safeguards and mechanisms **for mitigating those risks and** for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to newly established large scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

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

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

74) Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their rights or giving rise to unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of the processing activities. The supervisory authority should give advice where the envisaged processing might not be in compliance with this Regulation. The supervisory authority should respond to the request for consultation in a defined period (…). However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its duties and powers laid down in this Regulation. Such consultation should equally take place in the course of the preparation of a legislative or regulatory measure which provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing.

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

Article 33

Data protection impact assessment [1]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific[2] risks for the rights and freedoms of data subjects[3], the controller **(…)**[4] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[5]. **The controller shall ask where necessary the processor for assistance when carrying a data protection impact assessment.**

---

1 ES, HU and UK scrutiny reservation; FR thought that the possible application to public/private archives required further scrutiny.

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

3 BE scrutiny reservation.

4 Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deletion.

5 ES had proposed exempting certified processing operations. BE, CZ, EE and had proposed exempting a controller who had appointed a DPO.

1a **The controller shall seek the advice of the data protection officer when carrying a data protection impact assessment.**

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

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[1] are based that produce legal effects concerning data subjects or severely affect data subjects[2];

(b) data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale[3];

(c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (…)[4];

---

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

2 FR thought profiling measures might need to be covered by this Article, but this type of processing is largely covered by paragraph 2(a).

3 DE proposed referring to 'particularly sensitive personal information, in particular special categories of personal data under Article 9(1), data on children, genetic data or biometric data'. FR and IT are also supportive of the inclusion on sensitive data.

4 BE, FR, SK and IT asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale'. DE proposed the following text: 'processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where legitimate expectations are not met, for example owing to the context of the processing operation'.

(d) personal data in large scale processing systems containing genetic data or biometric data[1];

(e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects[2].

2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board. [3]

2b. Prior to the adoption of the list the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [4]

---

1 COM reservation on deletion of reference to children. DE proposed 'processing operations which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons'.

2 BE and DE reservation: in favour of deleting this subparagraph. NL and PL thought a role could be given to the EDPB in order to determine high-risk operations.

3 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

4 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks for rights and freedoms of data subjects, the measures envisaged to address the risks[1], safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[2], taking into account the rights and legitimate interests of data subjects and other persons concerned[3].

4. (…)[4]

5. Where a controller is a public authority or body[5] and where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[6].

6. (…)

7. (…)

---

1 DE suggests adding ' also in view of Article 30'.

2 NL proposes to specify this reference and refer to Articles 30, 31, 32 and 35.

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

4 BE, FR indicated that this was a completely impractical obligation. NL and COM were in favour of maintaining it.

5 BE proposed replacing the criterion of a controller being a public body by 'data are processed for the public interest'.

6 IT scrutiny reservation. DK, IT and COM think the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

Article 34

Prior (…) consultation[1]

1. (…)

2. The controller (…)[2] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a high degree of specific risks[3] [4]. **The controller shall ask where necessary the processor for assistance with respect to the consultation of the supervisory authority.**

---

1 ES, HU and UK scrutiny reservation; DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. See revised recital 74, which clarifies the scope of the obligation.

2 Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deleting processor.

3 FR and SE scrutiny reservation on the concept of a high degree of specific risks. It was pointed out that such assessments might be time-consuming. IT thought there should be scope for consulting the DPA in other cases as well.

4 DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller (…)[1]. This period may be extended for a further **six weeks**, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay[2].

4. (…)

5. (…)[3]

6. When consulting the supervisory authority pursuant to paragraph 2, the controller (…) shall provide the supervisory authority ~~,~~ with

(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

---

1 Drafting amended in order to take account of the concern expressed by several delegations that a sanctioning power for DPAs would be difficult to reconcile with (1) the duty on controllers to make prior consultation under the previous paragraph (DE, DK, NL, SE, SI) and (2) the freedom of expression (NL, PL, SI).

2 ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing.

3 IT reservation on the deletion of paragraphs 4 and 5.

(c) **the measures and safeguards provided to protect the data subject pursuant to this Regulation;**

(d) **where applicable , the contact details of the data protection officer;**

(e) the data protection impact assessment **as** provided for in Article 33 and

(g) any (…) **other** information requested by the supervisory authority (…).[1].

7. Member States shall consult the supervisory authority during the preparation[2] of proposals for legislative or regulatory measures which provide for the processing of personal data and which**, in particular,** may severely[3] affect categories of data subjects by virtue of the nature, scope or purposes of such processing. **The supervisory authority shall respond to consultation requests in due time**.

7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[4].

8. (…)

9. (…)

---

1 DE thought this paragraph should be deleted.

2 CZ wanted clarification that this obligation does not apply to private member's bills.

3 COM reservation, in particular regarding regulatory measures: this threshold is not present in the 1995 Directive.

4 DK, NL, PL, SE scrutiny reservation.

Article 37

Tasks of the data protection officer

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

   (a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation (…);

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

   (c) (…)

   (d) (…)

   (e) (…)

   (f) **to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;**

   (g) to monitor responses to requests from the supervisory authority and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;

   (h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter[1].

2. (….)

_____

[1] FR suggested adding an obligation to draft an annual report on his activities, but this may be too heavy an obligation.