COUNCIL OF THE EUROPEAN UNION

Brussels, 31 January 2014

5880/14

Interinstitutional File: 2012/0011 (COD)

LIMITE

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

A. DATA PROTECTION IMPACT ASSESSMENTS

I. Background

1. Directive 95/46/EC provides for a general obligation to notify processing of personal data to the supervisory authorities (Articles 18 and 19). The proposed Regulation shifts away from this approach moving from an ex-ante notifications to an approach reinforcing the responsibility of controllers and processors (increased accountability) : the notification obligation is abolished, and replaced by procedures and mechanism which focus instead on processing operations likely to present specific risks to the rights and freedoms of data subjects.

2. Article 33 of the proposed Regulation requires the controller or processor to carry out a data protection impact assessment prior to the processing, including the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance.

3. Discussions have shown that there is support for data protection impact assessment. Some Member States have been expressed concerns as regards the costs associated with mandatory data protection impact assessments, in particular as regards SMEs. This relates to the scope of the data protection impact assessment and to the requirement to seek the views of data subjects which were considered as burdensome and unrealistic in light of the business constraints.

II. Content of the current presidency compromise text

4. In order to better link impact assessments with an enhanced risk-based approach, the following changes have already been introduced to the Commission's proposal:

- Only the controller is obliged to carry out a data protection impact assessment (as opposed to an obligation imposed also on the processor) (Article 33(1));
- The scope concerns processing "likely to present specific risks" to the rights and freedoms of data subjects (Article 33(1)). The list of processing that present specific risks is exhaustive and covers four situations (decisions based on profiling, sensitive data for taking decisions, public monitoring on a large scale, biometric and genetic systems on a large scale).
- Specific clarifications have been provided as regards the covered processing (Article 33(2)):
    - Processing concerning "a systematic and extensive evaluation of personal aspects relating to a natural person" is linked with the notion of profiling on which decisions are based that produce legal effects or severely affect data subjects (Article 33(2)(a));

- The list of sensitive data has been aligned to Article 9(1) (Article 33(2)(b));
- The monitoring of publicly accessible places has to be "on a large scale" (Article 33(2)(c));
- The reference to "filing systems" has been replaced with large scale "processing systems", and the reference to children has been removed (Article 33(2)(d));
- The wording on the possibility for supervisory authorities to indicate other processing operations which are likely to present specific risks for the rights and freedoms of the data subjects has been simplified (Article 33(1)(e)). In addition, the compromise provides that the supervisory authorities should establish a public list of the kind of processing that have to undergo an impact assessment and communicate it to the European Data Protection Board, triggering the consistency mechanism in certain situations (Article 33(2a) and (2b));

- Furthermore, the compromise specifies that public authority controllers are exempted from a data protection impact assessment. Not only processing necessary for compliance with a legal obligation are exempted but also those necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The exemption applies for processing based on Union law and Member State law. Member States keep the option of carrying out a data protection impact assessment in those cases if they wish to do so (Article 33(5);
- The obligation for the controller to seek the views of data subjects or their representatives on the intended processing was deleted;
- The possibility for the Commission to adopt delegated and implementing acts was deleted.

III. Further considerations

5. The current provision on data protection impact assessments ensures that only processing operations which are likely to present specific risks undergo a thorough analysis.

6. In light of the previous DAPIX discussions, it could be envisaged to align Article 33(1)(a) with the new wording of Article 20 (now entitled "Automated processing and profiling").

7. Following the discussions on obligations of controllers and processors, it might be helpful to provide for a certain role of support for the processor when the controller is conducting the data protection impact assessment. It could therefore be envisaged to specify that the processor should assist/support the controller in ensuring compliance with the obligations pursuant to Articles 33 and 34.

8. If a controller has designated a data protection officer, it might be envisaged to state in the text that the data protection officer should be involved/kept informed of the data protection assessment.

9. *In this context, the Presidency therefore invites delegations to express their views on:*

   a. *Whether they support the compromise reached on the issue of data protection impact assessment ;*

   b. *Building on this compromise,*

      i. *specify that the processor should assist the controller in ensuring compliance with the obligations pursuant to Articles 33 (data protection impact assessment) and 34 (prior consultation) ;*

      ii. *Ensure the information/involvement of the DPO in the impact assessment process.*

B. PRIOR CONSULTATION

I. Background

10. Article 20 of Directive 95/46/EC requires a prior checking of determined processing operations "likely to present specific risks to the rights and freedoms of data subjects", involving an examination prior to the start of these processing operations. Such prior checks are to be carried out either by the supervisory authority following receipt of a notification from the controller, or by the data protection official who in cases of doubt must consult the supervisory authority. Following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing.

11. Article 20(3) of Directive 95/46/EC equally provides that the prior checking required by the Directive could take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards. Correspondingly, Article 28(1) obliges Member States to consult with supervisory authorities when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

12. Article 34 of the Commission's proposed Regulation imposes on the controller and the processor an obligation to carry out a prior consultation with the supervisory authority to cases where either

- a data protection impact assessment (as provided for in Article 33) indicates that processing operations are by virtue of their nature, their scope or their purposes, "likely to present a high degree of specific risks" (Article 34 (2)); or

- where the supervisory authority deems it necessary to carry out such a prior consultation on processing operations that are "likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes" (Article 34 (2)(b)), on a basis of a list to be made public Article 34 (4)).

13. The proposed Regulation also requires consultation of the supervisory authority in the preparation of legislative measure to be adopted by the national parliament (Article 34 (7)) and the corresponding duty for the supervisory authority (Article 52(1)(f)).

14. Discussions have shown that there is support for a requirement of prior consultation. However concerns have been expressed as regards the capacity of supervisory authorities to deal with these consultations, questioning the need for obliging the processor to consult, and in general on the practical effects of such consultation (timing, outcomes, etc.).

II. Content of the current presidency compromise text

15. In order to better demarcate these provisions the following changes have been introduced to the Commission's proposal:

- The provisions on prior authorizations which were limited to situations involving third country transfers have been moved to Chapter V (cf. Articles 42(2)(d), 42(5));
- The obligation to consult with the supervisory authority rests now only upon the controller, not the processor (Article 34(2));
- Prior consultation is now limited to residual risk cases, that is where the outcome of a data protection impact assessment referred to in Article 33 indicates that the processing, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, is likely to present a high degree of specific risks to the rights and freedoms of data subjects (Article 34(2));
- Recital 74 adds further illustrative examples requiring such prior consultation, other than excluding individuals from their right, or by the use of specific new technologies, namely: "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";
- The practicalities of prior consultations have been further circumscribed (Article 34(3),(6)), including deadlines;

- The consultation of the supervisory authority during the preparation of legislative or regulatory measures has been limited to those measures which may "severely affect categories of data subjects by virtue of the nature, scope or purposes of such processing" (Article 34(7)) and the corresponding duty for the supervisory authority in Article 52(1)(f) has been deleted;
- A possibility for Member States to require a prior authorization by a supervisory authority has been introduced for tasks carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health (Article 34(7a));
- The possibility for the Commission to adopt delegated and implementing acts in this areas was deleted (Article 34(8) and (9)).

III. Further considerations

16. As regards the consultation of the supervisory authority during the preparation of legislative or regulatory measures which provide for the processing of personal data, in order to highlight this specific situation, but without unnecessarily restricting the scope of such consultation with the supervisory authorities, the text could be clarified by inserting “in particular,” before “may severely affect categories of data subjects by virtue of the nature, scope or purposes of such processing”.

17. In addition, a corresponding duty for supervisory authorities to respond to such consultation requests by Member State, with timeframes etc. might be specifically added.

18. In this context, the Presidency invites delegations to express their views on:

a. *Whether they support the compromise reached on the issue of prior consultation as referred to in point 15 above; or*

b. *As an alternative, whether they consider that, building on this compromise, the text of Article 34(7) should be clarified as referred to in points 16 and 17 above*.