COUNCIL OF THE EUROPEAN UNION

Brussels, 1 March 2013

6607/1/13 REV 1

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 18
JAI 125
MI 116
DRS 30
DAPIX 28
FREMP 13
COMIX 108
CODEC 359

NOTE

from:	Presidency
to:	Council
No. prev. doc.:	16525/1/12 REV 1 DATAPROTECT 132 JAI 819 DAPIX 145 MI 753 FREMP 141 DRS 131 CODEC 2744 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155 5779/13 DATAPROTECT 4 JAI 53 MI 47 DRS 18 DAPIX 8 FREMP 4 COMIX 44 CODEC 164
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) - Implementation of risk-based approach - Flexibility for the Public Sector

I. General

1. The purpose of this Presidency note is to report to the Council on the progress achieved on the Commission proposal for a General Data Protection Regulation. During the first six weeks of its term, the Presidency has devoted a total of ten working days to this file (seven meeting days in the Working Party on Information Exchange and Data Protection (DAPIX) and three in the Friends of the Presidency). This has allowed it, building upon the work accomplished by the Danish and the Cyprus Presidency, to finalise a first examination of the entire proposal.

The Presidency has also commenced the process of giving a follow-up to the instructions by the JHA Council at its December 2012 meeting regarding two important imperatives in the negotiations, namely injecting a more risk-based approach into the Regulation and checking whether and how the regulation can provide sufficient flexibility for the public sector.

II. Risk-based approach

2. In the course of the first examination of the proposal for a General Data Protection Regulation, several Member States have voiced their disagreement with the level of prescriptiveness of a number of the proposed obligations in the draft Regulation. At the same time, some others have recalled the need to guarantee legal certainty in the proposed Regulation.

3. The Cyprus Presidency had already invited delegations to give their views on alternative ways of reducing administrative burden while maintaining the protection of individual rights. Many delegations had stated that the risk inherent in certain data processing operations should be a main criterion for calibrating the data protection obligations. Where the data protection risk is higher, more detailed obligations would be justified and where it is comparably lower, the level of prescriptiveness can and should be reduced.

4. At its December meeting, the Council instructed the DAPIX Working Party to continue to work on concrete proposals to implement a strengthened risk-based approach in the text of the draft Regulation.

5. In accordance with this instruction the Presidency suggested amendments to the proposed Regulation as regards the text of Chapter IV (on the controllers' and processors' responsibility). The revised draft of this Chapter includes a 'horizontal clause' in Article 22 of the Regulation, accompanied by a risk-based redrafting of many provisions of this Chapter (especially articles 23, 26, 28, 30, 31, 33, 34 and 35). Provisions with limited value-added (articles 27 and 29) have been dropped. Whilst the Presidency's redrafting of Chapter IV[1] was generally welcomed, differences of approach remain in respect of certain articles:

---

[1] See Annex I to 5702/143 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155. This is subject to a general scrutiny reservation by delegations.

(a) While there is broad agreement on the need for data protection impact assessments where processing presents specific risks (Article 33), some Member States question the obligation to engage in prior consultation with the supervisory authority where such an assessment indicates that the proposed processing operations are indeed likely to present a high degree of specific risk. Processing could not then commence during the suggested consultation period.

(b) As regards the designation of a data protection officer, some Member States, while accepting the designation of a data protection officer in case of risky processing, nonetheless consider that designation should be optional rather than mandatory. Moreover, some benefit in terms of lighter obligations should apply in cases where such an officer is designated. This would help to incentivise the designation of such officers.

(c) While there is broad support for codes of conduct (Article 38) and certification mechanisms (Article 39), several Member States consider that there is scope for stronger linkages between these articles and the risk assessment process in earlier articles of Chapter IV. This would help to incentivise the application of approved codes and to promote wider use of approved data protection certification mechanisms. It could be envisaged that there is no need for further risk assessments where a controller follows a code of conduct or a category of processing operation benefits from a certification mechanism.

6. Discussions on the new draft of Chapter IV have shown that it needs to be further refined in order to establish criteria for distinguishing different types of risk that may entail different types of obligations on the controller taking account, inter alia, of the needs of micro, small and medium-sized enterprises (SMEs). Another element that needs to be further explored is whether, and if so how, the use of pseudonymous data can contribute to the calibrating of controllers' and processors' data protection obligations while maintaining protection levels.

7. Whereas Chapter IV of the Regulation offers most scope for a risk-based approach, the Presidency has also sought to inject elements of this approach into parts of Chapter III (in particular articles 12, 14 and 15) with a view to ensuring effective and efficient exercise of data subject rights, while improving certainty and transparency. It is proposed to drop certain provisions which are no longer required due to restructuring of the text (articles 11 and 13).

8. The Presidency sees no need for several provisions which would enable the Commission to adopt delegated acts and implementing acts, e.g. paragraphs 7 and 8 of article 14; paragraphs 3 and 4 of article 15; paragraph 4 of article 22; paragraph 3 of article 23 and paragraph 9 of article 34. Obviously this is without prejudice to the horizontal review of the merits of the empowerments for delegated and implementing acts throughout the Regulation that needs to take place at a later stage.

9. At the meeting of the DAPIX Working Party on 12 and 13 February 2013 the suggested changes to the proposed Regulation have been broadly welcomed by delegations. The Chair of the Working Party has indicated that the Presidency will seek to take account as far as possible of the written and oral remarks provided by delegations.

III. Flexibility for the public sector

10. At an early stage of the discussions several Member States stated that they need more flexibility regarding data protection rules for the public sector in order to enable them to apply these rules in the context of their constitutional, legal and institutional setup. At the July JHA Informal Ministerial Meeting in Nicosia, Ministers engaged in a debate on the application of data protection rules to the public sector and at the December JHA Council it was agreed that the question as to whether and how the Regulation can provide flexibility for the Member States' public sector, could not be decided until after completion of the first examination of the text of the draft Regulation.

11. Following the completion of a first examination, the Presidency has started the process of investigating whether and how the Regulation can take sufficient account of the specificities of the public sector in Member States. This debate raises difficult questions of defining the demarcating lines between the private and the public sector. It has emerged that there may be a need for tailoring the application of some data protection rules to take into account the specificities of the public sector (e.g. as regards public records / state archives; on profiling).

12. A possible avenue for allowing Member States to clarify the application of the Regulation's data protection principles to the specificities of their public sector is to make clear what type of details may be specified by the national - or, as the case may be, Union - law, by way of addition of appropriate text in relation to Article 6(3). It should be clarified that it should be for such national - or, as the case may be, Union - law to determine the purpose of the processing and the controller. Furthermore it should be clarified that such law could, within the limits of the Regulation, specify the type of data which are subject to the processing, those who are authorised to consult and use the data, purpose limitations, storage periods, and processing procedures. The principle of public access to official documents also needs to be taken expressly into account.

13. While the first discussions in the Friends of the Presidency meeting of 14 February 2013 demonstrated that there is a degree of flexibility already built into the revised draft of the Regulation, there is a need to further clarify the scope of this flexibility. Further work will reveal whether it is capable of accommodating the required level of flexibility for Member States' public sector and the matter is not therefore ripe for discussion at this Council meeting.

14. In view of the above, the Council is invited

1) to take note of the above state of play;

2) to discuss whether

(a) controllers should have an obligation to engage in prior consultation with the supervisory authority where their risk assessment indicates that envisaged processing operations are likely to present a high degree of specific risk,

(b) the designation of a data protection officer should be optional rather than mandatory and whether the controller's obligations can be alleviated in cases where a data protection officer is then designated on a voluntary basis,

(c) the application of approved codes of conduct and the use of approved data protection certification mechanisms should be incentivised by establishing linkages with the risk assessment process;

3) to instruct <u>COREPER and</u> DAPIX to continue work on the risk-based approach, inter alia, by

(a) further developing criteria for enabling the controller and processor to distinguish risk levels along the lines suggested in paragraph 6 above, in order to calibrate the application of their data protection obligations;

(b) further exploring the use of pseudonymous data as a means of calibrating controllers' and processors' data protection obligations; and

4) to instruct <u>COREPER and</u> DAPIX to continue work on flexibility for the public sector along the lines suggested in paragraph 12 above, by clarifying the details that can be regulated under the law that provides the national legal basis for the data processing.