PUBLIC

COUNCIL OF THE EUROPEAN UNION

Brussels, 15 January 2014

5345/14

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 5
JAI 23
MI 39
DRS 8
DAPIX 5
FREMP 5
COMIX 29
CODEC 92

NOTE

from:	Presidency
to:	Working Group on Information Exchange and Data Protection (DAPIX)
Subject:	Specific issues of Chapters I - IV of the General Data Protection Regulation - certain aspects of the relationship between controllers and processors

I. Background

1. During the 2013 June JHA Council, Ministers discussed key issues on the proposal for a Regulation setting out a general EU framework for data protection on the basis of a document prepared by the Irish Presidency (Council document 11013/13). Delegations generally welcomed the considerable progress achieved on the proposed Regulation under the Irish Presidency. On the understanding that no part of the proposed Regulation can be agreed until the whole text of the regulation is agreed, it was concluded that the amended text of Chapters I to IV was a good basis for further progress on the proposal for a Regulation. This has been maintained in the compromise text prepared by the Lithuanian Presidency (Council document 17831/13).

2. With this understanding, the Presidency proposed to focus the discussions of the Working Party on specific issues stemming from Chapters I-IV of the General Data Protection Regulation which require further consideration. A first discussion in the Working Party on 8-10 January 2014 dealt with pseudonymous data, and profiling (17971/13). In continuation of that discussion, the Presidency has prepared this paper in order to facilitate a discussion on certain aspects of the relationship between controllers and processors. Some delegations have questioned the provisions for obligations of processors deriving directly from the proposed Regulation (as opposed to mere contractual obligations). The allocation of liability between controllers and processors has also been raised by some delegations. The Presidency envisages the discussion of other related issues.

II. Relationship between controllers and processors

Content of the current presidency compromise text

Obligations of controllers

3. The proposed Regulation applies to and sets out the respective obligations for controllers and for processors: the large majority of obligations under the proposed Regulation only apply to controllers. Under the rules contained in Chapters I – IV (Council document 17831/13) a controller is obliged to :

- ensure compliance with principles relating to personal data processing (Article 5 and 6);
- demonstrate that unambiguous or explicit consent has been given by the data subject (Article 7(1) and Article 7 (1a));
- make reasonable efforts to verify that in relation to the offering of information society services to a child below the age of 13 years the consent is given or authorised by the child's parent or guardian – (Article 8(1) second subparagraph);
- take appropriate measures to provide information to the data subject (Article 14 and Article 14a) ;

- take appropriate measures as regards the right of access, the right to rectification, the right to be forgotten and to erasure, the right to restriction of processing, the right to data portability, the right to object (Articles 15 to 19);

- implement appropriate measures and be able to demonstrate (accountability) that the processing of personal data is performed in compliance with the Regulation, including by making recourse to data protection by design and by default (Article 22, Article 23);

- determine in a transparent manner the respective obligations for compliance with the Regulation in case of joint controllers (Article24);

- designate a representative in the Union if they are not established in the Union – (Article. 25);

- use only processors providing sufficient guarantees ensuring that the processing will meet the requirements of the Regulation(Article26);

- maintain a records of all categories of personal data processing activities and, on request, make it available to the supervisory authority (Article 28(1) and Article 28(3));

- implement appropriate measures as regards security of processing (Article 30);

- notify a personal data breach to the supervisory authority and the data subject (Article 31 and 32);

- carry out a data protection impact assessment under certain conditions (Article. 33);

- consult the supervisory authority where a data protection impact assessment indicates that a certain processing of personal data is likely to present specific risks (Article 34(1));

- take appropriate measures with respect to data protection officers (Articles 35 and 36);

- provide information to the certification body and allow it access to its processing activities (Article 39(3));

- adduce appropriate safeguards (e.g. by making use of binding corporate rules (BCRs) for processors, or standard data protection contractual clauses, or by obtaining an authorisation by a supervisory authority) for international data transfers (Articles 42-44);
- assess the circumstances of small scale international data transfers based on legitimate interests, and, where necessary, adduce suitable data protection safeguards (Article 44(1)(h)), and document such assessment and safeguards in records available to the supervisory authority on request (Article 44(6)).

Obligations of processors

4. While under the current Directive the processor is only referred to in the provisions concerning definitions and data security measures, the proposed Regulation establishes directly processor-specific obligations: Under the rules contained in Chapters I – IV (Council document 17831/13) processors are directly obliged to

   - process personal data only based on a contract or another legal act binding the processor to the controller (Article 26(2));
   - maintain records of categories of personal data processing activities carried out on behalf of a controller (Article 28(2a)) and, on request, make the record available to the supervisory authority (Article 28(3));.
   - ensure data security, having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, by way of appropriate technical and organisational measures (Article 30(1));
   - ensure that any person acting under the authority of the processor who has access to personal data shall not process them except on instructions from the controller (Article 30(2b));
   - alert the controller of a personal data breach (Article 31(2));

- respect the requirements for data protection officers, if a data protection officer is designated (Articles 35 to 37);
- provide information to the certification body and allow it access to its processing activities (Article 39(3));
- adduce appropriate safeguards (e.g. by making use of binding corporate rules (BCRs) for processors, or standard data protection contractual clauses, or by obtaining an authorisation by a supervisory authority) for international data transfers (Articles 42-44);
- assess the circumstances of small scale international data transfers based on legitimate interests, and, where necessary, adduce suitable data protection safeguards (Article 44(1)(h)), and document such assessment and safeguards in records available to the supervisory authority on request (Article 44(6)).

5. Some of the provisions mentioned above refer to both the controller and the processor:
   - making available to the supervisory authority records of all categories of personal data processing activities (Article 28 (3));
   - implement appropriate measures as regards security of processing (Article 30);
   - respect the requirements for data protection officers, if a data protection officer is designated (Articles 35 to 37);
   - provide information to the certification body and allow it access to its processing activities (Article 39(3));
   - adduce appropriate safeguards for international data transfers (Articles 42-44);
   - assess the circumstances of small scale international data transfers based on legitimate interests, and, where necessary, adduce suitable data protection safeguards (Article 44(1)(h)), and document such assessment and safeguards in records available to the supervisory authority on request (Article 44(6)).

6. The rules contained in Chapters I - IV must be read in close connection with other rules of the Regulation, in particular the rules on responsibility and liability foreseen in Chapter VIII: Article 77(1) of the proposed Regulation foresees that any person who has suffered damage as a result of a non-compliant data processing operation has the right to receive compensation from the controller or processor for the damage suffered. Moreover, where more than one controller or processor, or a controller and a processor are involved each of them are jointly and severally liable for the entire amount of the damage, with the possibility for internal recourse claims between controllers and/or processors, and an exemption of liability (Article 77(2) and (3)). Both controllers and processors are also under the supervision of the independent data protection supervisory authorities, with one supervisory for the main establishment of either the controller or the processor (under the rules contained in Chapter VI), and may be subjected to administrative fines (Articles 79 and 79a) and/or other penalties e.g. criminal sanctions if deemed necessary by a Member State (Article 80).

7. During the discussion, questions have arisen whether, and if so how, some of the respective obligations for and the relationship between controllers and processors could further be clarified.

8. To this effect the following aspects have been integrated in the compromise text of Chapters I to IV of the proposed Regulation in the compromise text (Council document 17831/13):

   - a specific provision according to which the sufficient guarantees to be adduced by a processor for international data transfers may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a making use of a certification mechanism pursuant to Article 39 (Article 26(1a));
   - an explicit reference to the fact that the carrying out of processing by a processor is to be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects (Article 26(2));

- a clear distinction between the obligations of the controller and processor to maintain records of categories of personal data processing activities (Article 28(1) and (2a)); The list applicable for data processors is reduced in comparison with that for the data controllers and concerns only the name and contact details of the processor and of the data protection officer, the categories of processing carried out on behalf of each controller and, where applicable, the categories of transfers of personal data to a third country;
- the removal of the data processor from the obligation to carry out data protection impact assessments or to consult with the supervisory authority prior to the processing in specific risky situations (Articles 33(1) and 34(2));
- enabling processors to making use of codes of conduct (Articles 38 and 28a) and of certification mechanisms (Articles 39 and 39a).

Further considerations

9. Whilst the discussions have shown that there is an overall support for the compromise text of Chapters I to IV of the proposed Regulation in the compromise text (Council document 17831/13), some Member States still point to the difficulties in determining the roles of controllers and processors, including those established outside the EU/EEA, in particular in the context of cloud computing where the controller (especially if it is a SME) may be in a difficult position to exercise control on the processed personal data and to ensure the follow up on how the cloud provider delivers the requested services.

   In some cloud computing scenarios, clients of cloud computing services may not be in a sufficiently strong position to instruct a processor and to negotiate the contractual terms of use of the cloud services, as standardised offers are a feature of many cloud computing services. Nevertheless, the imbalance in the contractual power of a small controller with respect to large service providers should not remove the responsibility of the controller who remains responsible to ensure that clauses and terms of contracts are in compliance with EU data protection law.

10. Some increased legal certainty could be achieved by explicitly specifying in the proposed Regulation that the required contract between the controller and processor under Article 26(2) could be based on a "standard contract" between the controller and the processor. The proposed Regulation already provides, as the current Directive, for the possibility to develop standard data protection clauses for international data transfers laid down in points (b) to (d) of Article 42(2):

- adopted either by the Commission in accordance with the examination procedure referred to in Article 87(2); or
- adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57, and subsequently adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or
- contained in approved and certified contractual clauses, authorised by a supervisory authority pursuant to Article 39.

In addition, the European Data Protection Board may issue non-binding guidelines or recommendations as to the application of the provisions applying to controllers and processors.

These existing mechanisms could therefore be generalised, and applied to situations within the EU/EEA. Among others, the CEN (European Committee for Standardization) has already developed a model to assist compliance with obligations imposed by Article 17 of the Data Protection Directive 95/46/EC (cf. CWA 15292:2005).

11. In this context, the Presidency invites delegations to:

a. Confirm that they support the repartition of obligations between controllers and processors in the current compromise as mentioned above under point 8, including the deletion of the processor from the obligations to carry out data protection impact assessments or to consult with the supervisory authority prior to the processing in specifically risky situations;

b. Whether, in addition, delegations favour specifying that the required contract between the controller and processor under Article 26(2) could take the form of a "standardized controller-processor-relationship contract", applying the same procedures as already foreseen under points (b) to (d) of Article 42(2), as referred to above under point 10.