COUNCIL OF
THE EUROPEAN UNION

Brussels, 23 May 2014
(OR. en)

9831/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 70
JAI 309
MI 422
DRS 66
DAPIX 63
FREMP 89
COMIX 262
CODEC 1289

NOTE

From:	General Secretariat of the Council
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) - Article 26 (Processor)

Delegations will find below comments regarding Article 26 (Processor).

TABLE OF CONTENT

CZECH REPUBLIC	**3**
SPAIN	**5**
FRANCE	**7**
ITALY	**10**
LATVIA	**12**
HUNGARY	**13**
POLAND	**14**
ROMANIA	**17**
SLOVAK REPUBLIC	**18**
SWEDEN	**19**

CZECH REPUBLIC

On Article 26 (Processor)

Comments on 5881/1/14 REV 1.

In general

As has been shown by the discussion at the DAPIX working party on 10 and 11 April, there are still grave problems in:

a) establishing a clear distinction between controllers and processors;
b) solving de-facto disproportionate dominance of certain processors over controllers;
c) avoiding disproportionate burden for SMEs;
d) overcome difficulties with chains of processors; and
e) avoid further complication of one-stop-shop principle as the jurisdiction becomes centered on enterprise rather than on processing.

Therefore CZ wishes to reiterate that it would be beneficial to abolish the special position of processors and to regard them as controllers in their own right (see footnote 210 in document 17831/13).

However, as the Presidency invited the Member States, CZ wishes to present following particular comments as well:

Article 26 paragraph 2

CZ supports the insertion of "other legal act" for the flexibility it affords while still insisting on its binding nature.

Article 26 paragraph 2aa

CZ agrees with the principle, but considers the formulation unfortunate as it appears to confuse obligation and result. It is not clear what happens when the obligations imposed on sub-processor are not the same – the first controller will be in breach of regulation, but what about the sub-controller and what about the validity of the contract?

It would be better to either (a) simply oblige the first processor to impose the same obligations on sub-processor by contract or (b) to impose the same by the Regulation itself.

Article 26 paragraph 2ab

CZ welcomes the fact that contract clauses are not obligatory.

Article 26 paragraph 3

The reference should be to paragraph 2aa rather than to 2a, as 2a does not elaborate on "other legal act".

SPAIN

Comments on Article 26: the processor

Art. 26.2.a)

(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject and in such a case, the processor shall notify the controller **unless Union law or the law of the Member State to which the processor is subject** prohibits such notification **on important grounds of public interest**;

We are worried that this paragraph may be read in a sense that allows the processor not only not to inform the controller about certain processing operations required by law, but also not to notify the controller the mere existence of a law that may impose the processor certain processing operations. This interpretation could be sorted out with the following approach:

(a) process the personal data only on instructions from the controller (…),-**and inform the controller of the existence of Union or Member State law that may impose other legal instructions for the processing of personal data. The legal act shall stipulate that the processor must inform of processing operations subject to instructions imposed by law, except when these laws expressly prohibit this notification.**

Comments on Article 18: Right to data portability

2. Where the data subject has provided personal data and the processing, (…) based on consent or on a contract, is carried on in an automated processing system [~~[provided by an information society service]~~], the data subject shall have the right to ~~withdraw~~ **dispose of** these data in a **commonly used format and** to **request the controller or processor to** transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn, **without prejudice to Article 17**.

The current version of this article does not clearly envisage two cases that in our opinion should be included within the scope of the right to data portability: the right of a data subject to request a controller to transmit the data to another controller(for example, a user requests Facebook to transmit all his or her pictures to Picasa), and the right to request the first controller to erase those data after transmitting them to the second controller (for example, a user requests Facebook to erase his or her pictures and transmit them to Picasa). In order for the right to data portability to answer to these cases, we propose the above wording for art. 18.2.

Article 26.1.d)

(d) determine the conditions for enlisting another processor (…), **such as a requirement of specific prior consent of the controller;**

We would word this paragraph in another way: (d) **enlist another processor only on the conditions explicitly defined in the contract and accepted by the controller**. The idea is the same, but we believe that this text clearly stresses that it is the controller who authorises the subcontracts that the processor might sign.

Article 26

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and in accordance with the examination procedure referred to in Article 87(2).

The fact that the Commission is competent to lay down these standard clauses is not coherent with the rest of the system. We understand that these particular clauses are just models or good practices, but not compulsory. Therefore, we find it unnecessary to burden the adoption of these clauses with the procedure established in art. 87.2. Perhaps it would be advisable to allow each Data Protection Authority to develop their own standard clauses, and use the consistency procedure to make them European-wide.

FRANCE

(a) Presidency proposal regarding Article 26 (Processor)

5881/1/14 REV 1 DATAPROTECT 15 JAI 48 MI 93 DRS 16 DAPIX 9 FREMP 14 COMIX 70 CODEC 232

First, the French authorities would stress that, from a civilian viewpoint, they are in favour of a clear division of responsibilities between the controller and the processor, in accordance with the conventional rules of civil law; from an administrative point of view and with regard to the supervisory authorities, however, they would suggest that the proposed Regulation establish a mechanism whereby those authorities could take action against the processor if the latter fails to comply with his obligations under the proposal. To that end, the provisions concerning the supervisory authorities should make express reference to the possibility of supervision and the actual penalties which those authorities may impose on processors.

We would point out that, in certain situations, processors have very considerable powers and responsibilities compared to controllers, who are powerless in the face of their processors' economic strength. It is also for this reason that we would like horizontal discussions to be organised on the subject of processors, going beyond the scope of Article 26.

As a further preliminary point, we would like to see the addition of a requirement for the processor to notify his controller of his dealings with the supervisory authority.

Moreover, we do not support the proposed editorial additions, in particular to recital 63a, insofar as they aim to legitimise the processing activities carried out by the processor by "transforming" him into a controller. The sole objective of those additions should be to ensure that a processor who acts other than as instructed by the controller may be held responsible in the same way as if he were himself the controller (thereby imposing a heavier burden on him).

While we are more in favour of an option imposing harsher penalties on processors, who are required to process data as instructed by the controller, we do not wish such individuals (and in particular the most powerful processors) to be allowed to legitimise their activities "*contra legem*" (since Article 26 prohibits them from processing data other than for the controller and as instructed by the latter), and thereby to become autonomous controllers with respect to data transmitted to them by a controller in connection with a specific contract (see below).

In terms of substance, we wish to make the following comments concerning the rewording of Article 26:

- we support the amendments clarifying that the processor will assist the controller in ensuring compliance with his obligations;

- with regard to the introductory section of paragraph 2, we have reservations about the concept of other, "non-contract-type" binding legal acts which would allow the use of processors, insofar as the aim is to avoid the requirement for a contractual relationship in all instances of processing. In that connection, we would ask once again for specific examples of situations in which that concept might apply, and wonder whether it might cover adhesion contracts, for example.

- in point (a) of the same paragraph, we note the explanations provided by the Presidency regarding the cases covered by the underlined text ("*and in such a case, the processor shall notify the controller unless the law prohibits such notification*"). At this stage, however, we maintain our reservation on this provision, which is intended to resolve, albeit elliptically, a conflict between national and European standards.

- with regard to new paragraph 2aa, we would like the wording of this paragraph to be clarified, at least in order to specify that it refers solely to data protection obligations; pending such clarification, we wish to enter a scrutiny reservation on this provision.

- with regard to paragraph 2b, we wish to enter a scrutiny reservation on this provision.

- with regard to paragraph 2c, we propose once again that the wording of this provision be amended as follows so as to allow the EDPB to adopt standard contractual clauses as well: "*A supervisory authority or the EDPB may adopt standard contractual clauses for the matters referred to in paragraphs 1 and 2 in accordance with the consistency mechanism referred to in Article 57*".
  In that connection, we would reiterate that we would like horizontal discussions to take place on the subject of the EDPB's role and powers.

- Finally, with regard to paragraph 3, we would query the meaning of the end of this paragraph ("*or other non-legible form which is capable of being converted into a legible form*"), which seems both too vague and overly detailed. We therefore enter a reservation on that wording.

Regarding the editorial additions to recital 63a, as proposed by the Presidency, we would recall our preliminary comments concerning the reclassification of the processor as a controller in cases where the former acts other than as instructed by the controller. In order to make it clear that the option of reclassification as a controller exists only in order to enable processors to be penalised more effectively, this part of the recital could be worded as follows:
"*The contract should also specify the duty for the processor to process personal data only on instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. If a processor processes personal data other than as instructed by the controller, th**is** processor should be **sanctioned for the infringement of this specific obligation laid down in Article 26 of this Regulation and in addition should be** considered as a controller in respect of that processing **and thus sanctioned as such for the other infringements of this Regulation.***"

We would also like to see a reference to the article concerning penalties in order to clarify that the processor will always be penalised for having acted other than as instructed by the controller.

Finally, we would stress that, if the sole aim of this provision is to increase the burden of responsibility on a processor who acts other than as instructed by the controller, then this point ought to be re-instated in Article 26(4).

ITALY

We agree on the amendments to recital 63a, in particular the obligation for the processor to return or delete the personal data; this is in line with the emphasis on accountability of processors as set forth elsewhere in the draft Regulation. However, we think it would be desirable to clarify – as regards the preceding sentence – that if a processor processes the data other than as instructed by the controller, the processing in question is unlawful and the processor shall be fully liable for it unless there is a legal basis for such processing. This is an important point to be made, as recent cases (like the SWIFT one) showed.

We would propose accordingly to add the following sentence:
"If a processor processes…….should be considered as a controller in respect of that processing; **in such case, the processing shall be unlawful and the processor shall be liable for it unless there is a legal basis under Union or Member State law justifying the processor's departing from the instructions."**

Article 26

2. [1]The carrying out of processing by a processor shall be governed by a contract **or other legal act[2] binding the processor to the controller**, 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 (…..) and stipulating in particular that the processor shall:

We agree on the text in bold, in particular as it clarifies that the "other legal act" must have the same features as the contract (it must be binding, set out subject matter, duration, nature, purpose of the processing, etc.).

[1] Some delegations (UK, IE) thought this requirement was too onerous for one-off transactions especially in the case of single traders/practitioners or SMEs who used services of a subcontractor.

[2] FR wanted to know what was meant by an 'other legal act'. SE thought a recital should clarify it could cover Member State legislation. AT suggested that the details referred to for the contract should also apply to 'other legal act'.

2a. **Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the other processor shall provide sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation.**

We support this amendment which is modelled after the mechanism in place for Binding Corporate Rules as developed by European DPAs. The safeguards applying to sub-processors, if any, should be the same as those applying to the processors appointed initially by the controller.

2ab. **Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2aa may be based, in whole or in parts[3], on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a[4].**

We fully support the concept of standard contractual clauses to regulate processor-controller relationships.

[3] ES suggestion.
[4] IE reservation.

LATVIA

a) In response to PRES question about Article 26:

Latvia considers that it is important to establish in the Regulation that between the controller and the processor should be legal connection,
for example, a contract or legal agreement, that sets the duties and responsibilities of controller and processor.

Latvia does not oppose to supplementing the Regulation with a condition that processor can process personal data for different purpose, not only the initial purpose, if the controller have agreed to it or if the national law provides for it.

Latvia considers that in PRES proposal of Article 26 the words “in particular” should be replaced with “where appropriate”, because Regulation is not a legal instrument that should provide the exact content of a contract.

Latvia considers that Regulation should include provisions that could be included in a contract, but leaving the possibility to determine the content of the contract to controller and processor.

HUNGARY

Presidency proposal regarding Art. 26 (Processor)

1. Concerning the Presidency's proposal regarding Art. 26 (Processor), Hungary would like to draw the attention to the following problems:

- The term *„actively process"* in the last sentence of recital (63a) is unclear, thus its application may lead to difficulties. Clarification or erasure of the term is therefore suggested.

- Albeit Article 26 of the draft Regulation has been in several respects improved, it still does not provide for sufficient clarity with regard to the legal status of the sub-processor. According to paragraph 2., legal relationship between the controller and the processor shall be established (a *"contract or other legal act binding the processor to the controller"*) while according to paragraph 2aa. it seems that the sub-processor will not be bound to the controller but to the "primary" processor instead. If that is the case, it should be clearly stated that the primary processor should be responsible vis-à-vis the controller for the operation of the sub-processor with the same conditions as this operation would be conducted by the primary processor itself (e.g. without enlisting another processor).

- In point (d) and (f) of para. 2 of Article 26 the term *"determine"* does not fit to the wording of the chapeau of para 2. *"the processor shall…"* as the conditions mentioned in these points are to be determined by the contract or other legal act regulating the relationship of the controller and the processor.

POLAND

DATA PROTECTION IMPACT AND PRIOR CONSULTATION

74a) The processor ~~**should**~~ **may** 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. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific risks for the rights and freedoms of data subjects, the controller **(…)** shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…). The controller ~~**shall**~~ **may** ask where necessary the processor for assistance when carrying a data protection impact assessment.

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 are based that produce legal effects concerning data subjects or severely affect data subjects;

(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;

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

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

(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.

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.

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.

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, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. (…)

5. Where a controller is a public authority or body 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. (…)

7. (…)

ROMANIA

Art 26 - Processor

With reference to the proposals referring to the concept/notion of processor, respectively regarding data protection impact assessment and prior authorisation, we consider that we can maintain the general observations expressed during the DAPIX meetings.

RO wishes to thank PRES for the work concerning the new changes on the provisions of Article 26 and we consider the detailed explanations referring to the responsibilities of the processor to be useful.

In the same time, RO appreciates the positive elements brought to the text as it is, for example, the elimination of the obligation of the processor to follow the procedure of prior consultation. It is part of the logic to improve the administrative procedures. This is one of the important innovations elements which the draft regulation brings to the current normative framework.

SLOVAK REPUBLIC

Controllers and processors

SK very positively welcomes new text which regulates relations between controllers and processors and we would like the PRES for these modifications. We also welcome elaboration obligations in the course of selecting another processor and current wording of the proposal more or less corresponds with our position towards so-called another processor.

We also consider it necessary to clarify first new sentence in recital No. 63a *„If a processor processes personal data other than as instructed by the controller, the processor should be consider as a controller in respect of that processing.“,* in a manner which shall clearly state that the processor must not process personal data in a manner other than as instructed by the controller and only after violation of such instructions the processor becomes new controller.

Similarly we deem it necessary to clarify "*another legal act"* ideally in the recital. Therefore we would like to be added to footnote No. 5 in the Art, 26(2).

We would also welcome addition that the another processor processes personal data on processors responsibility and that another processor is considered as processor. This should be amended in Art. 26(2a):

2a. Where a processor enlists another processor **(sub-processor)** for carrying out specific processing activities on behalf of the controller, the other processor **(sub-processor)** shall provide sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation. **Another processor (sub-processor) processes personal data and provides their protection on processor´s liability. Provisions of this Regulation regarding the processor are binding also for another processor (sub-processor). For the purposes of this Regulation another processor (sub-processor) is considered as the processor.**

We would also like to be added in footnote No. 1 in Art. 26(1).

SWEDEN

Bold italics indicate proposed new text.
~~Bold strikethrough~~ indicates proposed deletions.

Recital 63a

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated by means of adherence of the processor to a code of conduct or a certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act binding the processor to the controller, 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, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are either adopted by the Commission or by a supervisory authority in accordance with the consistency mechanism and adopted by the Commission, or which are part of a certification granted in the certification mechanism**~~. If a processor processes personal data other than as instructed by the controller, the processor should be considered as a controller in respect of that processing. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; in that case the processor should implement appropriate measures to ensure the security and confidentiality of the personal data and should not actively process the personal data anymore.~~**

Comment

SE believes that the latter part of this recital is difficult as it might lead to the conclusion that the Regulation in fact endorses processing outside the contract between the controller and the processor.

Article 26

Processor

1. (…) The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…) .

1a. The provision of sufficient guarantees referred to in paragraphs 1 and 2a may be demonstrated by means of adherence of the processor to a code of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller, 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 (…..) and stipulating in particular ***where relevant*** that the processor shall:

a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject and in such a case, the processor shall notify the controller unless Union law or the law of the Member State to which the processor is subject prohibits such notification on important grounds of public interest ;
b) (…)
c) take all (…) measures required pursuant to Article 30;
d) determine the conditions for enlisting another processor (…), such as a requirement of specific prior consent of the controller ;
e) as far as (…) possible, taking into account the nature of the processing , assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;

f) determine how the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34;

g) return or delete, at the choice of the controller, the personal data after the completion of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; ~~**in that case the processor shall implement appropriate measures to ensure the security and confidentiality of the personal data;**~~

h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article.

2a. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the other processor shall provide sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation.

2aa. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, in a contract or other legal act the same obligations shall be imposed on that other processor as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2.

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2aa may be based, in whole or in parts, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a .

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and in accordance with the examination procedure referred to in Article 87(2).

2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and in accordance with the consistency mechanism referred to in Article 57.

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.

4. (…)

5. (…)

Comments

To maintain the risk based approach of processing the suggested wording in par. 1 is better. The latter part of par. 2(g) is redundant since this already is stipulated in (c).