Council of the European Union

Brussels, 23 September 2014
(OR. en)

13505/14

LIMITE

DATAPROTECT 124
JAI 700
MI 694
DRS 117
DAPIX 130
FREMP 159
COMIX 482
CODEC 1864

Interinstitutional File:
2012/0011 (COD)

NOTE

From:	Austrian Delegation
To:	Delegations
No. prev. doc.:	12312/1/14 REV 1 DATAPROTECT 109 JAI 630 MI 579 DRS 104 DAPIX 109 FREMP 148 COMIX 403 CODEC 1675
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) - Chapter IV

The Austrian delegation thanks the Presidency for considering the Austrian proposals and submits annexed drafting suggestions.

ANNEX

Drafting suggestion by the Austrian Delegation
Chapter IV (Doc. 12312/1/14 REV 1)

Proposal for changes in Art. 22 – Obligation of the controller

1. Taking into account the nature, context, scope and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of data subjects, the controller shall (…) implement appropriate measures ***including such as the implementation of appropriate data protection policies*** *and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.*

2. For the purposes of para 1 the controller shall, prior to any processing of personal data, carry out a preliminary risk evaluation to establish the level of expected risk (low, medium or high risk). To this end the controller shall in particular take into account the lists published by supervisory authorities and the European Data Protection Board according to Article 33 para 2a and Article 33 para 2c.

~~2a. Where proportionate in relation to the processing activities , the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller .~~

Explanation and Justification
The obligation to make recourse to appropriate data protection policies should not be subject to a consideration artificially separated from the decision making process under Article 22 para 1 and in particular not be subject to differing criteria. We therefore propose to incorporate the core elements of Article 22 para 2a into Article 22 para 1.

In our view the functioning of para 1 of Article 22 presupposes that the controller first of all gives some consideration to potential risks stemming from the circumstances of the processing envisaged. In our understanding the changes in recital 60 point to an obligation for the controller to carry out such a "preliminary risk assessment". Consequently Austria, in pursuance of its written comments as documented in council document 12267/2/14, pp. 113, proposes to add a new para 2 to Article 22 setting out a respective explicit obligation.

This preliminary assessment would merely have to establish in which category of risk a planned processing operation would fall. More precise details on the preliminary assessment should be provided in section 3 of Chapter IV (see below).

Proposal regarding recital 61

AT proposes to add the following at the end of the current presidency proposal:

In the case of information society service providers such as for example internet search engines or online shops the collection of data of unregistered users aiming at recognizing or monitoring them when revisiting the respective website after having closed and reopened the internet browser would not be consistent with the principles of data protection by design an data protection by default. The same applies to methods applied by such service providers to assign different devices (e.g. terminal, cell phone etc) to a specific unregistered user having recourse thereto.

Explanation and justification
As the experience shows, the principles of data protection by design and by default are not yet sufficiently put into practice by software producers and service providers. In order to avoid that these principles lose any meaning, it deems necessary to include some practical example applications in the considerations.

for amendment to Art. 33

1. Where the processing, taking into account the nature, scope context, or purposes of the processing, is likely to result in a ***medium*** *specific risk for the rights and freedoms of data subjects, ~~such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage,~~ 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. (...).*

Para 2

0) [insertion of text deleted in para 1] ***the envisaged processing poses a specific risk for the rights and freedoms of data subjects such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage,***

Para. 2 (chapeau):

A data protection impact assessment referred to in paragraph 1 shall be required ***in particular*** *in the following cases:*

Justification

Austria urges to reinstate the wording “in particular” in para. 2 as some flexibility is required notably with a view to possible future threats to the rights and freedoms of data subjects resulting from enhanced technologies. Thus an illustrative list of criteria indicating a medium level of risk deems more appropriate.

Proposal for alternative/supplementary text of Article 33 para 2a, 2b and 2c

2a. The supervisory authority shall establish and make public an ***indicative*** *list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to Article 33 ("medium risk")* ***or for a prior consultation pursuant to Article 34*** *("high risk").* ***In addition, the supervisory authority shall draw up and make public a list of processing operations typically presenting a low risk ("standard applications"). To the extent appropriate the list of standard applications should specify purposes, categories of data processed, groups of recipients, maximum retention period and appropriate security measures.*** *The supervisory authority shall communicate those lists to the European Data Protection Board.*

2b. ***Prior to the adoption of the lists pursuant to paragraph 2a*** *the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list 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.*

2c. The European Data Protection Board may, at its own initiative, notably at the request of one of its members, establish that a specific processing of personal data is likely to result in a medium or high degree of risk for the rights and freedoms of data subjects or on the other hand should be considered a "standard application". The European Data Protection Board shall maintain a publicly accessible register of kinds of processing dealt with according to paragraph 2b or 2c including the outcome of the examination. Furthermore the European Data Protection Board shall publish an up to date overall list of kinds of processing published by the supervisory authorities pursuant to paragraph 2a.

Explanation and justification

Within this context Austria reiterates its proposal to enable and facilitate a so-called preliminary risk evaluation (see text proposal regarding Art 22 paragraph 2 above).
Austria thus proposes to include in Article 33 paragraph 2a the mechanism of indicative lists determining low-risk ("standard applications"), medium risk and high risk data processing operations. These lists could be prepared at first by the supervisory authorities in the Member States. The Austrian Data Protection Supervisory Authority has been successfully operating a like system for many years. Examples for low-risk ("standard applications") could include the personnel administration, costumer support etc. The European Data Protection Board however should be in the position to complement to these lists. In the interest of EU-wide transparency and an easy access for controllers both to the domestic lists and lists established by the European Data Protection Board should be ensured.

Recital 60c has to be changed accordingly.

Proposal for alternative/supplementary text of Article 34 para 2

The controller (…) shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 ***or lists published by a supervisory authority or the European Data Protection Board*** *indicate~~s~~ that the processing is likely to result in a high degree of ~~specific~~ risk and this risk cannot be mitigated by reasonable measures in terms of available technology and costs of implementation to be taken by the controller.*

Further comments on the text:

Art. 23 Para 2

Austria prefers to keep the word "necessary" in para. 2 (instead of "not excessive").

Art. 26 Para 1b

Austria points to the fact that this proposal both contradicts to the substance of Article 77 para 1 and misses the overall scheme of the directive proposal. Thus, Austria urges to delete para 1b. Besides the Presidency proposal would significantly weaken the position of the data subject.

As to Para 2 point e and f

Austria is opposed to the insertion of the expression "to the extent stipulated" as it would go against the goal of a harmonized EU standard of data protection.

Art. 30 – Security of processing

We ask for inserting a new Footnote at the end of paragraph one: AT: scrutiny reservation on the last half-sentence with a view to the need to further clarify the exact scope and meaning of the terms "encryption, anonymisation and pseudonymisation" of personal data.

Art. 31 – Notification of a personal data breach to the supervisory authority

As to footnote 78: (alongside BE, DE, PL) AT supports the deletion of para. 1a. This should be documented therein. See also justification as documented in council document 12267/2/14, p.115 ("point 12").

Art. 32 Para 1

The expression "breach of anonymity or pseudonymity" needs further clarification. Scrutiny reservation.

Art. 33 Para 2 subparagraph c

The following footnote should be added at the end of para c:

"*AT is of the opinion that the notion "large scale" is of little use and should be avoided in using it as sole basis for assessing the risks." For further justification see comments set out in council document 12267/2/14, pp. 116 (heading: Art 33(2) points b and c).*

Art. 37 – Tasks of the data protection officer

The following footnote should be inserted at the end of the heading of this Article.
"AT is of the opinion that even if the designation of the DPO is not mandatory anymore one should abstain from deleting several tasks of the DPO in order to maintain a harmonized level throughout the Member States."

Art. 38 – Codes of conduct

Austria fully supports the changes made in para. 1ab as we share the same view (the same goes for Art. 39 para. 1a).

Art. 38a – Monitoring of codes of conduct

The following text should be inserted in footnote 135:
"AT believes that the primary responsibility for monitoring codes of conduct should lie with the institution that produced the code of conducts."

Comments to the footnotes:

Austria requests the deletion of the second sentence in footnote 21.

Footnote 41 and the AT-reference in FN 45 are to be deleted.