COUNCIL OF THE EUROPEAN UNION

Brussels, 23 April 2013 (25.04)
(OR. en,fr)

8826/13

Interinstitutional File: 2012/0011 (COD)

LIMITE

DATAPROTECT 50
JAI 313
MI 321
DRS 80
DAPIX 75
FREMP 44
COMIX 256
CODEC 896

NOTE

from:	French delegation
to:	Working Party on Information Exchange and Data Protection
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a General Data Protection Regulation - The risk-based approach

The risk-based approach has already been discussed several times within the Working Party and in the Council. The French authorities share the opinion that controllers' obligations should be modulated according to the risks created by the processing operations.

However, a number of issues remain: the **concept of risk is poorly defined** and the criteria used to identify it should be made clearer. We would like to offer some suggestions on this point (I and Annex).

It remains very difficult to define risk, however. For that reason, we agree with the Presidency that we should look primarily towards **case-by-case methods of defining the risks** created by processing operations. We consider that these methods should meet two main criteria: **legal certainty** for controllers and **simplicity**. We therefore propose limiting the use of impact assessments (II) and generalising the list system (III).

I. Clarify the concept of risk

- **Ensure the technological neutrality of the Regulation**

We are very keen for the proposal for a Regulation to maintain technological neutrality without, of course, reducing legal certainty for controllers.

Thus, as we have stated on several occasions, we would like the criteria defining the "risks" to be included in the instrument in order to ensure a uniform interpretation of the word, which currently appears at different points in the proposal alongside a wide variety of qualifying terms.

- **Definition of "risk" criteria**

Although it is difficult to give a precise definition of risk, it is still possible to refer to certain criteria. We therefore propose to supplement recitals 60, 67 and 70 in order to clarify the different sources of risks, as well as the concepts of severity and likelihood (these suggestions can be found in the Annex).

Under the system proposed below, the supervisory authorities would be able to refer to the criteria in points (a), (b), (c) and (d) of Article 33(2), which would be reintegrated into Article 34, in order to establish a list of risky processing operations for which consultation of the supervisory authority would be obligatory (see below).

II. Limit the use of impact assessments

The systematic use of impact assessments as proposed by the Regulation has several drawbacks:

- **High cost:** especially for small and medium-sized enterprises. Although the proposal for a Regulation initially exempted SMEs from certain obligations, we consider that the risks represented by the processing are not dependent on the size of the controller (small and medium-sized enterprises play a significant role in digital innovation and regularly develop new types of data processing which can sometimes lead to a high degree of risk). We are therefore not in favour of this type of exemption.
- **Major uncertainties:** the responsibility for determining the need for an impact assessment lies with the controller, who must refer to the criteria in Article 33 in order to decide whether one must be carried out. Failure to fulfil this obligation carries extremely high fines. The risk in terms of legal certainty for the controllers is therefore a major one.
- **A cumbersome and illogical system:** when the processing operation concerns the categories in Article 33, it is likely to present a risk for the controllers. One may wonder, therefore, what added value an impact assessment brings when it is ultimately likely that the data protection authority will have to be consulted anyway.
- **Increased risk in comparison with third-country enterprises:** these enterprises, which have different data protection cultures and are located outside of the European Union for the rest of their activities, may not assess risks in the same way as European enterprises. The impact assessment system may therefore result in distortions of competition.

III. Alternative Proposal

We propose that the publication of lists, which was already provided for in the initial proposal and which can henceforth be found in Article 34(2a) and (2b), be broadened and replace the impact assessments. The current French system works in this way and allows the list to be updated regularly by the supervisory authority.

The system would then work as follows:
Where the processing operation appears on a list drawn up by the supervisory authority, the controller should refer the matter to the supervisory authority so that it can examine the measures that should be taken to ensure maximum security of processing in the light of the data protection rules. The supervising authority will be able, where necessary, to request additional information and on a case-by-case basis where required, to request that the processing administrator undertake an impact assessment which would both outline the potential risks and propose appropriate solutions. The lists will be drawn up by the supervisory authority with reference to the criteria listed in the recitals and to the examples of types of risky processing defined in the new Article 34 (see redrafting proposal in the annex using the criteria provided for in Article 33(2)).

In order to establish these lists, we propose distinguishing between public and private processing:

- **For processing private individuals' data**

The EDPS would establish, publish and regularly update a list of processing operations considered risky, and for which the controllers should consult the national data protection authority. Drawing up these lists at European level would ensure a homogenous approach across the EU. These lists could also apply to the controllers of third countries which have to designate a representative within the Union, thus reinforcing the European dimension of the Regulation as regards third States.

- For data processing by **public authorities**

In order to guarantee the necessary flexibility in the case of public data processing, it would be necessary to entrust each national data protection authority with establishing and publishing the list of public processing operations that are considered risky, for which the controllers of these processing operations should be obliged to consult their data protection authority.

This procedure has a series of advantages:

- **Simplicity:** a controller could consult the list to find out whether they should consult the supervisory authority or not.
- **Lower cost:** recourse to impact assessments would be reduced and would only be carried out on a residual basis and at the request of the supervisory authorities.
- **Security:** The supervisory authorities seem better placed than the controllers to list the categories of processing which present risks to data subjects and which should be the subject of a priori supervision, or at least of a dialogue between the controller and the supervisory authority. Allowing companies to assess alone the risks involved in their own data processing operations, in particular in the case of small businesses or new types of processing, would place the controllers at excessive risk.
- **Homogenous approach:** Referral to the EDPS would allow for a homogenised risk-based approach at EU level since only one list would be established and valid throughout the EU. Furthermore, in order to compile this list and keep it up-to-date, dialogue between the supervisory authorities would be necessary since they would encounter the controllers at national level during consultations. This system therefore allows feedback from experience of and a uniform approach to risky processing methods, not only internally but also vis-à-vis third countries. The pooling of experience by the 27 supervisory authorities would usefully enhance the coherent system already provided for by the proposal for a Regulation, while also preventing divergent case law when statements are made (and therefore pre-empting possible conflicts at the time of supervision).

IV. Clarify the distinction between "risks" and "security"

- Recourse to lists of data processing operations that are considered risky in order to determine which cases must be referred to the supervisory authority should not mean that the Regulation should abandon the concept of "risk".

- The authorities that establish the lists must have information on the concept of risk in the Regulation. Furthermore, this concept is used in other parts of the text (for example, when dealing with security breaches).

- Nevertheless, for the use of "risk" to be useful and not lead to legal uncertainty, the text should be made more precise.

- **Distinction between the security of processing ("ISS Risks") and "privacy" risks**

As it stands, the proposal for a Regulation does not seem to distinguish clearly between the concept of "security" of processing (Article 30) and that of "risks" to data subjects from the processing operations (Article 33).

The "ISS" risks refer to threats to the controller (for example, the risk of intruders in the systems and data theft etc.). The "privacy" risks are those threats to data subjects, i.e. the material, moral or physical damage to data subjects which could originate from various data processing malfunctions. The "ISS risks" are therefore a component of the "privacy" risks but differ from them.

The French authorities' proposal would therefore also allow this point to be clarified.

It should first of all be noted in Article 30 that the risk considered is that of the security of processing, and not the risk to data subjects.

In addition, this concept should be better defined. Indeed, it is the controllers' responsibility to guarantee the security of their data processing; by contrast, the supervisory authorities themselves seem better placed to identify the "privacy" risks to the data subjects, in conjunction with the potential ISS risks, when they are establishing the lists, carrying out checks and being faced with disputes.

Nevertheless, the "risks" to the security of processing (ISS) could equally be addressed on a more general level. In this sense, the French authorities advocate, in addition to the (optional) use of certification mechanisms, provided for in Article 30 of the proposal for a Regulation, that ENISA be entrusted with the development of security standards for the controllers.

This system would offer the same advantages as the system using lists of processing operations considered risky (European homogeneity, legal security, reduction of costs for the controllers).

ANNEX

Proposals for alternative wording for the recitals and the concept of risk

Amendments to the recitals are highlighted in yellow.

As regards the criteria for the concept of risk, the French authorities propose the following amendments to recital 60 which introduces the subject:

These amendments take up the comments made in the meeting document and make some corrections to achieve greater coherence with the Regulation (the replacement of "should" by "shall" in particular).

- Recital 60:

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller **shall** (…) be obliged **to implement appropriate measures to ensure and be able** to demonstrate the compliance of each processing operation with this Regulation **(…). Such risks exist where, taking into account the nature, scope and purposes of the processing and the different sources of risks, physical, material or moral damages can occur, for example by excluding individuals from their rights or from the control over their personal data, or giving rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by a professional secrecy regulated by Union or Member State law or any other economic or social disadvantage. Where personal data are processed on behalf of the controller, the implementation of such measures should include in particular to use only a processor providing sufficient guarantees to implement appropriate technical and organisational measures. Where the processing (…) according to the EDPB and data protection authorities, (…) represent specific risks for the rights and freedoms of data subjects, the controller or processor shall consult the competent data protection authority and carry out, prior to the processing and on request of the data protection authority, an assessment of the impact of the envisaged processing operations on the protection of personal data. Guidance for the implementation of such measures by the controller, especially as regards the identification of the risks, their assessment in terms of severity and likelihood, and catalogues of good practices to treat the risks, could be given in particular by approved codes of conduct, approved certifications or guidelines of the European Data Protection Board, by a data protection officer, or, where a data protection impact assessment indicates that processing operations involve (…) specific risks, by the consultation of the supervisory authority prior to the processing. If proportionate, the verification of the obligations of the controller may be carried out by independent internal or external auditors or by providing an approved certification.**

In general, in the recitals and possibly in the Regulation, the phrase "*taking into account the nature, scope and purposes of the processing*" could be replaced by the phrase "*taking into account the nature, scope and purposes of the processing* ***and the different sources of risks***".

The French authorities propose the following alternative wording for recital 67 corresponding to Article 31

- Recital 67:

A personal data breach may, if not addressed in an adequate and timely manner, result in adverse physical, material or moral effects on the individuals such as the exclusion of individuals from their rights or from the control over their personal data, discrimination, identity theft or fraud, financial loss, damage of reputation or any other economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred (…) the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

The French authorities propose the following alternative wording for recital 64a corresponding to Article 33

- Recital 64a:

In order to enhance compliance with this Regulation in cases where the processing, according to the EDPB and data protection authorities, represent specific risks for the rights and freedoms of data subjects, (…) the controller or the processor shall be responsible to perform a data protection impact assessment, on request of the data protection authority, to evaluate the nature as well as the severity and likelihood of these risks, taking into account the nature, scope and purposes of the processing and the different sources of risks. The outcome of the assessment shall be taken into account when determining the extent of the requirements, in particular when implementing appropriate measures to ensure and be able to demonstrate that the processing of personal data is in compliance with this Regulation.

The French authorities propose the following alternative wording for recitals 70 and 74 corresponding to Article 34

- Recital 70:

Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanisms which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, and which are mentioned for these reasons on the lists published by the EDPB and data protection authorities. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing on request of the data protection authority (…) in order **to evaluate the nature and the severity and likelihood of these risks, taking into account the nature, scope and purposes of the processing and the different sources of risks. It** should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Proposals for alternative wording for Articles 30, 33 and 34

Article 30 - Security of processing

SECTION 2

data SECURITY (…)

Article 30

Security (…) of processing [1] [2]

1. Having regard to the state of the art and the costs of their implementation, and taking into account the nature, scope and purposes of the processing and the risks (…) for the (…) security of the processing[3], the ENISA shall establish and publish security standards specifying the security measures to be implemented according to the different types of risks identified.

1. (…) The controller and the processor[4] shall, in accordance with the standards issued by the ENISA, implement appropriate technical and organisational[5] measures [including the use of pseudonymous data] to ensure a level of (…) security appropriate to the (…) risks referred to in paragraph 1a.

---

1 Several delegations (DE, FR, and IE) thought that more clarity was required as to what kind of risks for which actors were concerned. DE regretted the text of Article 17 of the 1995 Data Protection Directive had not been followed more closely. PT would have hoped for a more ambitious text. IT and UK pleaded in favour of an equivalent principle of data security in Article 5.

2 BE suggested adding a paragraph clarifying that the measures envisaged are covered by Article 6(1)(f). The Presidency thinks that this is superfluous in view of the legal obligation under the Regulation to take such measures.

3 FR suggested this be limited to the processing of sensitive data. FR also remarked that in this context the controller should rather evaluate security risks. Further clarification was required as what is to be understood by 'risk'

4 Several delegations thought that the controller should have the main responsibility (NO, NL, UK).

5 SK thought 'personal' measures should also be mentioned.

2. (…)[1].

2a. The controller may demonstrate compliance with the requirements set out in paragraph1 by means of a certification mechanism pursuant to Article 39.

2b. Any person acting under the authority of the controller or the processor shall be bound by an obligation of confidentiality[2], which shall continue to have effect after the termination of their activity for the controller or processor[3].

3. (…).

4. (…)[4].

Article 33 - Impact assessment

(…)

(…) Deleted and moved to Article 34

[1] ES doubted the added value of this paragraph; NL, thought that this paragraph should be better aligned to paragraph 1. Therefore paragraphs 1 and 2 have been merged. NL wondered whether it would be possible to envisage different classes of data processing operations according the risk involved. UK suggested inserting a reference to

[2] CZ queried where this obligation would be defined.

[3] FR was examining any possible conflict with national labour laws and queried what was the link to Article 84.

[4] Deleted in view of comments made by DE, ES, IT, LV, RO and UK. PL was in favour keeping the empowerments of paragraphs 4 and 5.

Article 34 - Prior consultation

SECTION 3

(…) PRIOR AUTHORISATION AND DATA PROTECTION IMPACT ASSESSMENT

Article 34

Prior (…) consultation [1] [2]

1. (…)[3]

2. The European Data Protection Board shall establish and make public a list of the kind of processing which present specific risks, taking into account the nature, scope or purposes of the processing, for the rights and freedoms of data subjects[4], and for which the controller shall consult the supervisory authority, prior to the processing[5]. This list shall be reviewed on a regular basis as often as necessary and at least every year.

(…) (…) 2a. When establishing this list, the EDPB shall in particular address the following processing operations (…) presenting specific risks as referred to in paragraph 2:

---

1 DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. The Presidency has revised the wording of recital 74 with a view to clarifying the scope of the obligation.

2 BE suggested Article 34a: "*Member States may submit the processing of personal data concerning health, employment, social security and other by a public authority or body to a prior authorisation by a DPA to prevent misuse of crossing data and to protect data subject rights*".

3 At the suggestion of several delegations (IT, SI, UK) this paragraph was moved to Article 42(6).

4 BE scrutiny reservation. De would have preferred to refer to the right to data protection.

5 Addition so as to align the drafting to that of recital 70: GR.

(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on automated processing and on which decisions[1] are based that produce legal effects concerning (…) data subjects or **adversly** affect data subjects[2];

(b) information on sex life, health, race and ethnic origin **(…),** where the data are processed for taking **(…)** decisions regarding specific individuals on a large scale[3];

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (…)[4] on a large scale[5];

(d) personal data in large scale **processing** systems **containing** genetic data or biometric data[6];

(e) other operations where (…) the competent supervisory authority considers that the processing is likely to present specific risks for the fundamental rights and freedoms of data subjects[7].

---

1 BE proposed to replace this by wording similar to that used for profiling in Article 20: 'decision which produces adverse legal effects concerning this natural person or significant adverse effects concerning this natural person'. DE and NL also thought the drafting could be improved.

2 FR thought profiling measures might need to be covered by this Article, but the Presidency thinks this type of processing is largely covered by paragraph 2(a).

3 DE proposed referring to 'particularly sensitive personal information, in particular special categories of personal data under Article 9(1), data on children, genetic data or biometric data'. FR and IT are also supportive of the inclusion on sensitive data.

4 Reference to video-surveillance dropped in order to make the text more technology-neutral.

5 BE, FR, SK and IT asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale'. DE proposed the following text: 'processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where legitimate expectations are not met, for example owing to the context of the processing operation'.

6 COM reservation on deletion of reference to children. DE proposed 'processing operations which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons'.

7 BE and DE reservation: in favour of deleting this subparagraph. NL thought a role could be given to the EDPB in order to determine high-risk operations.

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation[1] (…) prohibit the intended processing and make appropriate recommendations to the data controller or processor[2]. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay[3].

3a. During the period referred to in paragraph 3, the controller [or processor] shall not commence processing activities[4]. After that period, if the supervisory authority has prohibited the processing or issued recommendations pursuant to paragraph 3, this authority shall expressly authorise the controller to commence the processing activities if the processing complies with this Regulation.

4. (…)

5. (…) [5]

6. **When consulting the supervisory authority pursuant to paragraph 2,** the controller or processor[6] shall provide the supervisory authority, on request, with a data protection impact assessment and any (…) information **requested by** the supervisory authority **(…)**[7].

---

1 BE suggestion. IT reservation on 6-weeks period.

2 SI reservation on the veto power of the DPA. Several delegations (DE, DK, NL, SE, SI) remarked that this sanctioning power was difficult to reconcile with the duty on controllers to make prior consultation under the previous paragraph. It was pointed out that this might lead to controllers avoiding to undertake data protection impact assessments. Several delegations (NL, PL, SI) queried how this veto power could be reconciled with the freedom of expression.

3 ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing. The Presidency thinks that any discussion regarding differentiating the DPA powers should take place under Article 53.

4 BE, NL and PL reservation: this would amount to making the consultation into an authorisation and result in uncertainty for companies

5 IT reservation on the deletion of paragraphs 4 and 5.

6 BE was opposed to mentioning the processor here.

7 DE thought this paragraph should be deleted.

6a. 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[1], safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[2], taking into account the rights and legitimate interests of data subjects and other persons concerned[3].

6b. Where a controller is a public authority or body[4] and where the processing pursuant to point (c) **or (e)**[5] of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, the supervisory authority shall establish and make public a list of the kind of processing for which the controller shall consult the supervisory authority[6].

7. Member States shall consult the supervisory authority during the preparation[7] of (…) legislative (…) measures which provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing (…).

---

1 DE suggests adding 'also in view of Article 30'.

2 NL proposes to specify this reference and refer to Articles 30, 31, 32 and 35.

3 DE and FR scrutiny reservation. DE referred to Article 23(b) of the 2008 Data Protection Framework Decision, which requires prior consultation of the DPA where 'the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.'

4 BE proposed replacing the criterion of a controller being a public body by 'data are processed for the public interest'.

5 DE and FR proposal.

6 COM thinks the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

7 CZ wanted clarification that this obligation does not apply to private member's bills.

7a. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 6b or the legislative measure referred to in paragraph 7 would not comply with this Regulation, in particular where risks for the rights and freedoms of data subjects are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation[1] (…) make appropriate recommendations to the data controller or processor[2] and publish these recommendations. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay[3].

[8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2[4].]

9. (…)

---

1 BE suggestion. IT reservation on 6-weeks period.

2 SI reservation on the veto power of the DPA. Several delegations (DE, DK, NL, SE, SI) remarked that this sanctioning power was difficult to reconcile with the duty on controllers to make prior consultation under the previous paragraph. It was pointed out that this might lead to controllers avoiding to undertake data protection impact assessments. Several delegations (NL, PL, SI) queried how this veto power could be reconciled with the freedom of expression.

3 ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing. The Presidency thinks that any discussion regarding differentiating the DPA powers should take place under Article 53.

4 BG, FR, UK and DE pleaded for the deletion of paragraph 8. PL wanted to keep it.