COUNCIL OF THE EUROPEAN UNION

Brussels, 14 March 2013

6278/3/13 REV 3

LIMITE

DATAPROTECT 12
JAI 88
MI 102
DRS 22
DAPIX 16
FREMP 10
COMIX 86
CODEC 300

Interinstitutional File: 2012/0011 (COD)

NOTE

from:	General Secretariat
to:	Working Group on Information Exchange and Data Protection (DAPIX)
Nos prev. docs:	16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155
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)

Further to the invitation by the Presidency (CM 1160/13) delegations have sent in written comments on Articles 28-39 of Chapter IV of the 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.

The comments received at 8 March 2013 are set out hereafter.

TABLE OF CONTENTS

BELGIUM

Article 28 Documentation

1. Each controller **(…)** and, if any, the controller's representative, shall maintain documentation of all **categories of** processing activities under its responsibility.

BE welcomes the modification proposed by the Presidency. However, BE thinks that a recital is necessary to give a way of interpretation of "all **categories of** processing activities".

2. ***This*** *documentation shall contain (…)the following information:*

(a) the name and contact details of the controller, any joint controller or processor, and of the ***controller's*** *representative, if any;*

(b) the name and contact details of the data protection officer, if any;

[(c) the purposes of the processing [including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)];

(c)bis description of the legitimate interests pursued by the controller where the processing is based on point (f) of article 6(1);

(d) a description of categories of data subjects and of the categories of personal data relating to them;

(e) the ***(…)*** *categories of recipients of the personal data* ***(…)****;*

(f) where applicable, ***the categories of*** *transfers of* ***personal*** *data to a third country or an international organisation,* ***(…)*** *and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;*

(f)bis in the case of a transfert to a third country on the basis of articles 42 and 43, the legally binding instrument

(g) a general indication of the time limits for erasure of the different categories of data;

(h) ***(…)***

(i) The name and contact details of the processor, if any

The aim of all the modifications is to be more precise and clear.

5. (new) When it is impossible or involve disproportionate efforts, the controller and the processor and, if any, the controller's representative, may not maintain or give to the supervisory authority the information referred to in §3 but shall motivate the reasons of the impossibility or of the disproportionate difficulty.

BE wants to take into account the case where it is impossible to maintain or give all the element of the documentation to the supervisory authority. In that case, the controller may justify reasons why the information cannot be given for example if there is a computer crash.

Article 30 Security and confidentiality of processing

2a. The obligation of confidentiality on any person acting under the authority of the controller or the processor shall continue to have effect ***during 5 years*** after the termination of their activity for the controller or processor

BE thinks that the obligation of confidentiality should be limited to 5 years. An obligation of confidentiality shouldn't last for a lifetime (that is different for an obligation of professional secrecy).

2 bis (new) The implementation by the controller and the processor of measures, as referred to in paragraphs 1, and the execution thereof which would require processing of certain data to increase network and information security, falls under article 6 (1) f.

BE thinks that the implementation by the controller of measures referred into §1 of the article 30 and the execution thereof may require the processing of certain data. In that respect, this processing should fall under article 6 (1) f of the regulation.

Article 31 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach ***which is likely to adversely affect the fundamental rights and freedoms of data subject,*** *the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.*

The notification shall not be required if the controller has applied appropriate measures to the data concerned by the personal data breach making that the breach has no consequences for the data subject.

BE wants to decrease the administrative burden and propose to add that if the controller has applied appropriate measures to the data concerned by the personal data breach making that the breach has no consequences for the data subject, the notification shall not be require.

Furthermore, BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" is not clear.
Indeed, BE believes that Chapter III of the draft regulation contains the core rights for data subjects and those rights need to be exercise without proving a prejudice. In that case, the controller has an obligation of result.
It is not the same for Chapter IV which is based, for the controller, on an obligation of means. The data subject has to prove a prejudice.
Therefore, BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject"* could cover a lot of things.
BE has a scrutiny reservation on this wording.

REM: Art. 4.3 of the e-privacy Directive (2002/58/EC modified by a directive of 2012) says that: "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual."
This wording is too broad and obliges the notification of all minor data breach.

3. The notification referred to in paragraph 1 must at least:

(a) describe the nature of the personal data breach including the categories and ***the approximate*** *number of data subjects concerned and the categories and number of data records concerned;*

BE tries to decrease the administrative burden. Concerning the point (a), BE believes that it is impossible to give the exact number of data subject concerned.

BE wants to delete the paragraphs 5 and 6 of the article 31. There is unanimity within the Council.

Article 32 Communication of a personal data breach to the data subject

1. When the personal data breach ***is likely to adversely affect the protection of the personal data or privacy of the data subject****, the controller shall, communicate the personal data breach to the data subject without undue delay.*

BE wants to decrease the administrative burden and propose to limit the obligation to communicate the personal data breach to the data subject only when this personal data breach is causing a significant prejudice to the data subject.
BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" is not clear.
Indeed, BE believes that Chapter III of the draft regulation contains the core rights for data subjects and those rights need to be exercise without proving a prejudice. In that case, the controller has an obligation of result.
It is not the same for Chapter IV which is based, for the controller, on an obligation of means. The data subject has to prove a prejudice.
Therefore, BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" could cover a lot of things.
BE has a scrutiny reservation on this wording.

REM: Art. 4.3 of the e-privacy Directive (2002/58/EC modified by a directive of 2012) says that: "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual."
This wording is too broad and obliges the notification of all minor data breach.

3. Notwithstanding paragraph (1), the communication of a personal data breach to the data subject shall not be required if the controller (…)has implemented appropriate technological protection measures and **(…)** those measures were applied to the data **affected by** the personal data breach. Such technological protection measures shall ~~*include those that*~~ ***have the purpose to*** render the data unintelligible to any person who is not authorised to access ~~***it***~~ ***them taking into account the nature of the data, the state of the art and the cost*****, such as encryption or the use of pseudonymous data**.

All the modifications have as consequence that the controller has an obligation of means and not an obligation of result.
It is impossible to have an obligation of result in this matter. The most protected computer system of the world remains always "breakable". It's only a question of time and means for the hacker.

BE wants to delete the paragraphs 5 and 6 of the article 32. There is unanimity within the Council.

SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTORISATION

Article 33 Data protection impact assessment

BE thinks that this article increases the administrative burden. In that respect, BE proposes to limit it to processing that present a specific risk.

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific risks for the fundamental rights and freedoms of data subjects, the controller ***or the processor acting on the controller's behalf*** *shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to processing the data.*

BE thinks that there is confusion between the obligation and responsibilities of the controller and the processor. The relationship between the controller and the processor should be reviewed in the entire regulation.

1a. Paragraph 1 shall not apply where a data protection officer has been designated in accordance with Article 35*(4).*

BE believes that the exemption to perform a data protection impact assessment should apply to all cases of appointment of a DPO, that means to the entire article 35 and not only the 35.4.

*2. The following processing operations **exhaustively** present specific risks referred to in paragraph 1:*
*(a) a systematic and extensive evaluation **on a large scale** of personal aspects relating to natural persons which is based on automated processing and on which decisions are based to produce legal effects **concerning data subjects or significantly affect data subjects**;*
*(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals **on a large scale**;*
*(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) **on a large scale**;*

BE considers that this paragraph is not clear. There is a lack of predictability. BE asks COM to make the list of the processing presenting a specific risk exhaustive.

Concerning the point (a): BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" is not clear.
Indeed, BE believes that Chapter III of the draft regulation contains the core rights for data subjects and those rights need to be exercise without proving a prejudice. In that case, the controller has an obligation of result.
It is not the same for Chapter IV which is based, for the controller, on an obligation of means. The data subject has to prove a prejudice.
Therefore, BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" could cover a lot of things.
BE has a scrutiny reservation on this wording.

REM: Art. 4.3 of the e-privacy Directive (2002/58/EC modified by a directive of 2012) says that: "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual."
This wording is too broad and obliges the notification of all minor data breach.

Concerning the point (a),(b) and (c): What's the meaning of « *on a large scale* »? This is totally unclear.

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 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 in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union.

BE has a scrutiny reservation on articles 2a and 2b. BE is not in favour to give this competence to the DPA's. Moreover the consistency mechanism is, for the moment, too long.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the 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.

BE has a scrutiny reservation on this paragraph 3.

5. Where ***~~the controller is a public authority or body~~*** ***the data are processed for the public interest*** *and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law* ***or the law of the Member State to which the controller is subject****, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.*

BE welcomes the modification proposed by the Presidency.
BE thinks that the notion of "public authority or body" is too narrow. BE proposes to use the notion of "*the data are processed for the public interest*".
This modification has a consequence:
BE wants to add a recital which stipulates that "the public interest depends of the interpretation made by the MS"

~~**6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium sized enterprises.**~~

BE wants to delete this paragraph.

Article 34 Prior authorisation and prior consultation

2. The controller ~~***or processor acting on the controller's behalf***~~ *shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in article 33 indicates that the processing is likely to present a high degree of specific risks.*

BE thinks that there is confusion between the obligation and responsibilities of the controller and the processor. The relationship between the controller and the processor should be reviewed in the entire regulation.

2 bis. Member states may submit by law the processing of personal data by public or private institutions who execute a task of public interest, such as the contribution to the application of the social security or to the execution of public health, to the prior authorization, in order to avoid processing which gravely affects the data subject's fundamental rights.

This is a particularity of the Belgian system of data protection. Our DPA is divided is several comities which may give their prior authorisation concerning several matters.
BE requests then the creation of a point 2bis as it is already states in the footnote 105.

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 period of maximum 6 weeks following the request for authorisation prohibit the intended processing and make appropriate recommendations to the data controller ~~***or processor***~~*.*

BE thinks that there is confusion between the obligation and responsibilities of the controller and the processor. The relationship between the controller and the processor should be reviewed in the entire regulation.

~~***3a. During the period referred to in paragraph 3, the controller [or processor] shall not commence processing activities.***~~

BE thinks that this paragraph risks to increase the administrative burden.
Either it is a consultation; in that case the controller may begin the processing;
Either it is an authorization; in that case the controller may not begin the processing.

BE wants the deletion of this paragraph.

6. When consulting the supervisory authority pursuant to paragraph 2, the controller ***~~or processor~~*** *shall provide the supervisory authority, on request, with the data protection impact assessment provided for in Article 33 and any information requested by the supervisory authority.*

BE thinks that there is confusion between the obligation and responsibilities of the controller and the processor. The relationship between the controller and the processor should be reviewed in the entire regulation.

SECTION 4 DATA PROTECTION OFFICER

Article 35 Designation of the data protection officer

1. The controller and the processor ***~~shall~~ may*** *designate a data protection officer where:*

BE considers that the function of DPO's should be a self-regulatory one and is not in favour of a mandatory designation of the DPO. See note 113.

(…)

(b) the processing is carried out by an enterprise employing ***250 persons*** *or more;*

Or

(c) the core activities of the controller or the processor consist of processing ***activities*** *which,* ***represent risks for the fundamental rights and freedoms of data subjects by virtue of the nature, scope or purposes of the processing***

BE thinks that:
- the criteria of 250 employees is not sufficient (see note 114)
- BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" is not clear.
Indeed, BE believes that Chapter III of the draft regulation contains the core rights for data subjects and those rights need to be exercise without proving a prejudice. In that case, the controller has an obligation of result.
It is not the same for Chapter IV which is based, for the controller, on an obligation of means. The data subject has to prove a prejudice.
Therefore, BE thinks that the wording "*which is likely to adversely affect the fundamental rights and freedoms of data subject*" could cover a lot of things.
BE has a scrutiny reservation on this wording.

REM: Art. 4.3 of the e-privacy Directive (2002/58/EC modified by a directive of 2012) says that: "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual."
This wording is too broad and obliges the notification of all minor data breach.

7. ***(…) The data protection officer shall be designated*** *for a period* ***appropriate to the processing activities of the controller or processor****.* ***(…)****. During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned* ***which justify the dismissal of an employee or civil servant****, be dismissed only* ~~***if the data protection officer no longer fulfils the conditions required for the performance of his or her duties***~~ ***for the positions expressed and the tasks accomplished in the performance of their duties.***

For BE the criteria on the base of which a DPO may be dismissed should not be based on the fulfilment of the conditions but on the positions expressed and the tasks accomplished for the performance of their duties.
See footnote 120.

9. ***Upon request,*** *the controller or the processor shall* ***make available*** *the name and contact details of the data protection officer to the supervisory authority* ***(…)***. ***Any modification of data protection officers' identity during their mandate, particularly in case of early resignation or as soon as their dismissal is envisaged, must also be notified to the supervisory authority.***

The aim of all the modifications is to be more precise and clear.

10. Data subjects ***~~may~~*** *contact the data protection officer on all issues related to the processing of the data subject's data and* ***the exercise of their*** *rights under this Regulation.*

BE considers that the "*may*" is not necessary.

11. ***~~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 the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5~~***

BE wants to delete this paragraph.

Article 36 Position of the data protection officer

2 bis: "The data protection officer must ensure confidentiality of information obtained while performing his or her tasks, in particular as regards to information relating to complaints and information relating to the data processing activities of the controller or processor."

BE disagrees with the analysis of the Presidency concerning the footnote 125. Indeed, article 30 is only applicable to the controller and the processor.

Article 37 Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following functions:

*(a) to inform and advise the controller**, ~~or~~** *the processor* ***and the employees who have to process personal data*** *of their obligations pursuant to this Regulation and to document this activity;*

(b) to monitor ***compliance with the regulation*** ~~***the implementation and application of this Regulation and of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations, and the related audits***~~

The aim of all the modifications is to be more precise and clear.

SECTION 5 CODES OF CONDUCT AND CERTIFICATION

Article 38 Codes of conduct

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission ***and the European data protection board****.*

BE thinks that the EDPB should also be informed. This modification has a consequence: addition of a point (h) in article 66: "*The European Data protection Board shall ensure the consistent application of this regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:* *(…)* ***h) Examine codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to article 38, paragraph 3."***

Article 39 Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall ***be voluntary, capable of global application and affordable. These mechanisms shall also be technology neutral and shall*** *contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.*

BE thinks that a certification scheme may help to encourage organisations to provide additional safeguards to personal data transferred out of the Union. The amendment proposed above would introduce important conditions on certification schemes that would ensure they are widely usable by controllers and processors large and small. Specifically, certification schemes would need to:

- *Be* ***voluntary***. Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections.
- *Be capable of being* ***rolled-out and recognised globally***. To help reduce the compliance burden on providers, any certification scheme should be capable of being endorsed by regulators in third countries as well as by those in the Union.
- *Be* ***affordable***. Some privacy certification regimes involve costs of upwards of €150,000 simply to certify one feature of a product or service. These costs create barriers to entry for all but the largest service providers, and discourage wide-scale use of the regime.
- Be **neutral as to system, service or technology**. Similarly situated services and products should be subject to the same assessment criteria. Favouring some solutions over others creates market distortions and hinders innovation.

BULGARIA

Article 28

Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. The documentation shall contain at least the following information:

   (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

   (b) the name and contact details of the data protection officer, if any;

   (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

   (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

   (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

   (g) a general indication of the time limits for erasure of the different categories of data;

   (h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) (….)[1]

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. (….)

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29

Cooperation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall cooperate, on request, with the competent supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

[1] Not relevant since the natural person in t his case is not considered as a data controller in relation to Art. 2, Para.2, Item (d) of the proposal.

SECTION 2
DATA SECURITY

Article 30

Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. (…)[1]

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

   (a) prevent any unauthorised access to personal data;

   (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

   (c) ensure the verification of the lawfulness of processing operations.

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

[1] Guidelines by EDPB to be provided.

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal severe[1] data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a severe personal data breach.

3. The notification referred to in paragraph 1 must at least:

   (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

   (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

   (c) recommend measures to mitigate the possible adverse effects of the personal data breach;

   (d) describe the consequences of the personal data breach;

   (e) describe the measures proposed or taken by the controller to address the personal data breach.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

[1] A new definition is needed as to the severity of the data breach. We suggest the following: "severe breach" means a breach of security affecting high number of individuals or of prevailing public interest.

5. (…)

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. (…)[1]

[1] Provide very detailed provision in the Regulation instead.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 34

Prior authorisation and prior consultation

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

   (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

   (b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. (…)[1]

9. (…)[2]

[1] Detailed provision in the Regulation instead.
[2] Difficult to unify the procedure on this matter.

SECTION 4
DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body; or

   (b) the processing is carried out by an enterprise employing 250 persons or more; or

   (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects

   (d) the impact assessment analysis demonstrates the necessity thereof

   (e) the processing affects more than 10 000 individuals.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject’s data and to request exercising the rights under this Regulation.

11. 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 the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating with the supervisory authority at the latter's request or on the data protection officer's own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

(i) to undergo a training provided by the supervisory authority.

2. (…)

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;

(b) the collection of data;

(c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights;

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

4. (…)[1]

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

[1] It is appropriate for the relevant supervisory authority to have competence to issue compulsory instructions and guidelines with regard to the Codes of Conduct.

CZECH REPUBLIC

As requested on 8 February, the comments are made in relation to document 5702/13.

CZ focuses on Articles only, as the recitals would have to be adapted later.

In general

CZ wishes to point out that comments given below are without prejudice to horizontal questions and issues, such as delegated and implementing acts or legal form of the proposal. Given the fact that these horizontal issues are being discussed separately, CZ did not specifically comment e.g. on provisions establishing implementing or delegated powers.

Article 28

- before letters (e)-(g) of the second paragraph a chapeau should be inserted:

"and, unless such cases are negligible in relation to whole extent of data processing:"

This would enable the controller to refrain from documenting very rare and specific operations that involve small amounts of personal data (such as transmission of some personal data of top management to third country, where the owner resides, once per several years). This would decrease administrative burden on the controllers.

- Paragraph 4 is supported, letter c) should be amended:

"categories of processing activities which are unlikely to represent serious risks for the fundamental rights and freedoms of data subjects by virtue of the nature, scope or purposes of the processing;"

CZ does not agree entirely with deletion of 4(b), as larger enterprises may bear the burden more easily. Still, CZ is able to support shift to risk-based approach in this matter.

Article 30

- Paragraph 2a should be amended:

"The controller or processor shall impose legally binding obligation of confidentiality on any person taking part in processing personal data under their authority (…); this obligation shall continue to have effect after the termination of their activity for the controller or processor."

CZ believes that the requirement to establish obligation of confidentiality should be spelled out expressly in the first place. As certain persons acting under the authority of processors and controllers would not be processing personal data in any meaningful way, it is not necessary to impose confidentiality on them.

Article 33

- Paragraph 1a is supported but should be amended to cover also Art. 35(1):

"Paragraph 1 shall not apply where a data protection officer has been designated in accordance with Article 35~~(4)~~."

CZ believes that data protection officer designated in accordance with Article 35(1) is even better suited to discover specific risks than DPO designated by association representing controllers.

Article 34

- Paragraph 7 should be amended:

Member States shall consult the supervisory authority during the standard preparation of (…) legislative or regulatory measures, or schemes based on such measures, which provide for the processing of personal data which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing (…) in order to ensure compliance of the intended processing with this Regulation; ~~such measures may concern the activities of public authorities and bodies, including those relating to health, employment and social security~~.

CZ has several concerns in this regard.
First, while CZ public administration always consults DPA on legislation prepared, there are other subjects empowered by Constitution to propose laws, such as Senate or individual MPs. They do not use this right frequently; however they frequently use their right to amend proposals submitted by the government. These instances should not trigger the need for (another) consultation round. Therefore, the word "standard" is proposed and it may be further clarified in recital.
Second, the use of semicolon at the end of sentence must be changed in order for the sentence to make sense.
Third, the end of sentence is probably superfluous and could be deleted.

Article 35

- In paragraph 1 letter (a) should be amended:

"the processing is carried out by or for a public authority or body, or"

CZ proposes to cover also natural and legal persons that fulfil public tasks for and on behalf of public authorities and bodies, either on the basis of a contract, or on a basis of legislation.

- In paragraph 1 letter (b) should be deleted.

CZ believes that it should be up to private enterprises to choose ways to ensure compliance with the Regulation, be it data protection officers, legal advice from lawyers etc.

- If 1(b) is kept, then:
  - it should be worded as follows:

"the processing involves large number of data subjects and is carried out by an enterprise employing 100 persons or more, or"

  - paragraph 2 should be redrafted to allow all controllers and processors to appoint a single data protection officer:

"In the case referred to in point (b) of paragraph 1, a group of ~~undertakings~~ controllers and processors may appoint a single data protection officer."

Large number of data subjects is better criterion of importance of data processing for the enterprise, while 100 persons decreases the threshold to capture even smaller enterprises that process personal data intensively.
Change of paragraph 2 should provide flexibility to e.g. enterprises that process personal data on small scale, but may require data protection officer with specialist knowledge or abilities. The duty to support DPO under Article 36(3) is strengthened by second sentence, thus preventing many enterprises hiring single DPO that would not be able to perform his or her tasks.

- Paragraph 7 should enable hiring DPO for unlimited period of time:

"The data protection officer shall be designated for unlimited time period (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her duties. "

CZ prefers unlimited period of time, as short terms might have a chilling effect on DPO's discharge of tasks when DPO wishes to renew his appointment.

GERMANY

By letter dated 15 January 2013 the Presidency invites the Member States to submit by, 8 February 2013, proposals for amendments and comments - apart from those already submitted in DAPIX - on Articles 28 to 39 of Chapter IV of the Commission proposal for a General Data Protection Regulation.

A. Preliminary remark

Germany thanks the Presidency for this opportunity to state its position. The proposals set out below should be seen as provisional, non-exhaustive contributions to further discussion of the legal act. Germany expressly reserves the right to submit further comments, including on general matters which concern all articles, such as detailed arrangements for the Commission's powers for delegated and implementing acts. Drafting suggestions and comments on the German-language version will follow at a later stage. Germany will comment on the recitals separately. As a precaution, additional comments made by Germany in DAPIX are included in its position and sometimes repeated below.

B. Comments on Articles 28 to 39

I.

General scrutiny reservations and reservations on individual provisions, as submitted in DAPIX and in the position on Articles 28 to 39, remain.

II.

1. re Article 28:

Article 28 ***Documentation*** 1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	*Article 28* ***Documentation*** 1. Each controller, (…) [and the controller's representative, if any] shall maintain documentation of all categories of processing operations under its responsibility[1]
2. The documentation shall contain at least the following information: a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	2. The documentation shall contain (…) the following information: a) the name and contact details of the controller, or any joint controller or processor, and of the representative <u>and data protection officer</u>, if any;

[1] Depends on the further development of Article 25, in particular whether and to what extent the representative is competent for processing data.

b) the name and contact details of the data protection officer, if any;	(…)
c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
d) a description of categories of data subjects and of the categories of personal data relating to them;	d) a description of categories of data subjects and of the categories of personal data relating to them;
e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	e) the recipients or categories of recipients of the personal data; (…)

f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	f) where applicable, transfers of data to a third country or an international organisation; (…)
g) a general indication of the time limits for erasure of the different categories of data;	g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).	h) a general description which allows the technical and organisational measures referred to in Article 30(1) to be evaluated.
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	(…)

4.	The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: a) a natural person processing personal data without a commercial interest; (…) orb) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	4.	The obligations referred to in paragraphs 1 and 2 shall not apply to <u>processing operations which, by virtue of their nature, scope or purposes, do not adversely affect the data subject's legitimate interests</u>[1] [2] (…). (…)
5.	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 the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.		(…)

[1] The risk-based approach should be included in other articles which do not form part of this position, e.g. Article 22. Furthermore, an attempt should be made to express the objectives of the General Data Protection Regulation more clearly, namely to prevent the misuse of personal data through identity theft and fraud, for example.

[2] In Germany's view, natural persons under point (d) of Article 2(2) should be excluded as far as possible. This would also settle the question of the exemption in point (b) of paragraph (4).

6.	The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or	(…)

2. re Article 29:

	Article 29 ***Cooperation with the supervisory authority***	(…)
1.	The controller and the processor and, if any, the representative of the controller, shall cooperate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	

2.	In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	(…)

3. re Article 30:

Article 30 ***Security of processing***	*Article 30* ***Security of processing***
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. The controller and the processor shall, with respect to the processing operations under their responsibility and having regard to the state of the art, implement the appropriate technical and organisational measures required for protection of confidentiality or for protection against accidental or unlawful destruction, accidental loss, unauthorised alteration, dissemination or access, or against any other form of unlawful personal data processing. In doing so, it is necessary to ensure an appropriate level of security whereby the effort is proportionate to the risks to the data subjects' right to personal data protection represented by the processing, by virtue of its nature, scope and purpose.

2.	The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.	(…)
3.	The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.	(…)

4.	The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to: a) prevent any unauthorised access to personal data; b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

4. re Article 31:

Article 31 ***Notification of breaches to the supervisory authority***	*Article 31* ***Notification of breaches to the supervisory authority***
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	1. In the case of a personal data breach, where there is a risk that the data subjects' rights or legitimate interests will be severely affected, in particular in the case of identity theft or fraud, damage to reputation or any other significant economic or social disadvantage, the controller shall notify the supervisory authority competent pursuant to Article 51 without undue delay after having become aware of it. Under the law of the Member State, any notification made by a person required to notify may only be used against him or her or against a person entitled to withhold evidence in criminal or administrative proceedings with that person's agreement.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. The processor shall notify the controller without undue delay after having become aware of a personal data breach. [1]
3. The notification referred to in paragraph 1 must at least: a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	3. The notification referred to in paragraphs 1 and 2 must at least: a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned; b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

[1] In view of the Commission proposal of 7 February 2013 for a Directive concerning measures to ensure a high level of network and information security across the Union (COM(2013) 48 final), it should be checked whether in certain cases the authority competent for network and information security should also be notified.

c) recommend measures to mitigate the possible adverse effects of the personal data breach; d) describe the consequences of the personal data breach; e) describe the measures proposed or taken by the controller to address the personal data breach.	c) <u>where possible</u>, recommend measures to mitigate the possible adverse effects on the <u>data subjects</u>; d) describe the <u>possible</u> consequences of the personal data breach; e) describe the measures proposed or taken by the controller to address the personal data breach.
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches, <u>taking into account their severity, by means of an appropriate</u> description of all facts surrounding the breach, its effects and the remedial action taken. (…)

5.	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 establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	(…)
6.	The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

5. re Article 32:

Article 32 ***Communication of a personal data breach to the data subject***	*Article 32* ***Communication of a personal data breach to the data subject***
1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. As soon as appropriate measures have been taken to render the data secure or where such measures were not taken without undue delay and there is no longer a risk for the criminal prosecution, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).	2. The communication to the data subject (…) shall (…) contain at least the information (…) provided for in points (b) and (c) of Article 31(3) as well as a description of the nature of the personal data breach in generally comprehensible terms.

3.	The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3.	The communication of a personal data breach to the data subject shall not be required if the controller demonstrates (…) to the supervisory authority that it implemented appropriate technological protection measures for the data concerned by the personal data breach at the time of the data breach, in particular state of the art encryption procedures which render the data unintelligible to any person who is not authorised to access it. Nor shall communication be required if the controller demonstrates to the supervisory authority that as a result of subsequent measures taken, the data subjects' rights and freedoms are no longer at risk. Where communication to the data subjects would involve disproportionate effort, in particular owing to the number of cases involved, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.	Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	(…)
5.	The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.	(…)
6.	The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

6. re Article 33:

Article 33 ***Data protection impact assessment***	*Article 33* ***<u>Data protection impact assessment</u>***
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	1. Where processing operations <u>may</u> present <u>particular</u> <u>risks</u>, <u>by virtue of their nature, scope or purposes</u>, to <u>th</u>e right of data subjects <u>to personal data protection,</u> the controller (…) shall, <u>for its area of responsibility</u>, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1: a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	2. The following processing operations <u>may</u> <u>present</u> specific risks referred to in paragraph 1: a) [processing of personal data intended to assess the data subject's personality, including his/her skills, performance <u>or behaviour</u>];[1]

[1] The detailed drafting depends on the discussions on Article 20.

b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	b) particularly sensitive personal information, in particular special categories of personal data under Article 9(1), data on children, genetic data or biometric data;
c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;	c) 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.

d) personal data in large scale filing systems on children, genetic data or biometric data;	d) processing operations involving personal data 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.
e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	e) [1] (…)
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the 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.	3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, also in view of Article 30, 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 (…).

[1] The Presidency proposal re point (e) of Article 33(2) and the new paragraphs 2a and 2b (the former paragraphs 4 and 5 of Article 34) requires further examination.

4.	The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	4.	The controller shall carry out the assessment at the request of the data subjects without prejudice to the protection of commercial or public interests or the security of the processing operations and make it available in an appropriate form.
5.	Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	5.	Where the controller is a public authority or body and the processing pursuant to points (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State, paragraphs 1 to 4 shall not apply unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6.	The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	(…)	

7.	The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

7. Re Article 34:

Article 34 ***Prior authorisation and prior consultation*** 1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.	*Article 34* ***Prior consultation*** [1] (…)

[1] Comments relating to the retention of the authorisation referred to in point (d) of Article 42(2) and Article 42(5) are provided in our comments on Chapter V.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where: a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	2. The <u>data protection officer referred to in Article 35(1) shall be responsible for carrying out the data protection impact assessment described in Article 33</u> and in <u>cases of doubt</u> shall consult the supervisory authority in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects, <u>in so far as</u>: a data protection impact assessment as provided for in Article 33 indicates that processing operations present <u>particularly high</u> risks. (…)

3.	Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.	(…)
4.	The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	(…)
5.	Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	(…)

6.	The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	(…)
7.	Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall provide that the supervisory authority is to be consulted during the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, designed to protect natural persons during the processing of personal data and to ensure the free movement of such data, in order to ensure compliance with this Regulation and other data protection provisions and in particular in order to mitigate the risks involved for the data subjects.

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.	(…)
9.	The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

8. Re Article 35:

Article 35 ***Designation of the data protection officer***	*Article 35* ***Designation of the data protection officer***
1. The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body; or b) the processing is carried out by an enterprise employing 250 persons or more; c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	1. The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body; or [b) the processing is carried out by an enterprise employing 250 persons or more, or] [1] the controller or processor performs processing operations which, by virtue of their nature, scope or purposes, present particularly high risks or which are necessary in accordance with point (f) of Article 6(1) for the purposes of the legitimate interests of a third party.

[1] For Germany it is important to maintain its own regulations, which involve a much lower personal threshold and different counting method, hence point (a) of paragraph 11. We would also maintain our criticism of the threshold value, which is too high (99.8 % of undertakings would be exempt) and the counting method (staff employed, rather than staff involved in the processing of personal data). Incentives to appoint a data protection officer could consist of simplified procedures for transfers to third countries as indicated in Chapter V, having regard to this when fixing the amount of the fine referred to in Article 79(2) or an additional step in the procedure to remedy non-compliance before the imposition of sanction, similarly to Article 79(3).

2.	In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2.	A group of undertakings may appoint a single data protection officer, if those undertakings act as a single unit for the purposes of contact with the outside world, if they regularly rely on processing within the group of undertakings and if the data subjects are not disadvantaged by the existence of a single data protection officer.
3.	Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3.	Where the controller or the processor is a public authority or body, the data protection officer may be designated for several public authorities or bodies, taking account of the organisational structure and size of the public authority or body.
4.	In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4.	Without prejudice to paragraph 1, the controller or processor may designate a data protection officer in order to comply with the rights and obligations under this Regulation.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37, <u>particularly the absence of any conflict of interests</u>. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	(…)

7.	The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	7.	The controller or the processor shall designate a data protection officer for a period of at least four years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if, under the law of the Member State, there are important grounds to justify dismissal of their contract without notice or if they no longer fulfil the conditions required for the performance of their duties, as indicated in paragraph 5. During their term of office, and for one year thereafter, their employment relationship may not be terminated, unless, under the law of the Member State, there are important grounds entitling the controller to terminate their contract without notice.
8.	The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8.	The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract. In so far as the data protection officer, in the course of his or her activities, obtains data in respect of which the management or persons employed by the controller are entitled, on professional grounds, to withhold evidence under the law of the Member State, that right shall also apply to data protection officers and their staff.

	Whether or not this right is exercised shall be the decision of the person entitled to withhold evidence for professional reasons. Insofar as the right to withhold evidence enjoyed by the data protection officer continues to apply, the relevant documents shall be the subject of a prohibition of confiscation under the law of the Member State.
9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	(…)
10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects may at any time contact the data protection officer on all issues relating to the processing of their personal data. The data protection officer shall be required to keep confidential the identity of the data subject and any circumstances allowing their identity to be inferred, unless indicated otherwise by the data subject.

11. 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 the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	11. The Member States may, by law: a) stipulate that controllers or processors, are required to designate a data protection office in cases other than those provided in point (b) of Article 35(1); b) specify the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

9. re Article 36:

Article 36 ***Position of the data protection officer***	*Article 36* ***Position of the data protection officer***
1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	2. The controller or processor shall ensure that the data protection officer performs the (…) tasks independently and does not receive any instructions as regards the exercise of the function. He shall not be penalised for performing his tasks. The data protection officer shall act under the direct (…) authority of the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the (…) tasks referred to in Article 37 and maintain the expert knowledge referred to in Article 35(5).

10. re Article 37:

Article 37 ***Tasks of the data protection officer***	*Article 37* ***Tasks of the data protection officer***
1. The controller or the processor shall entrust the data protection officer at least with the following tasks: a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;	1. The controller or the processor shall entrust the data protection officer at least with the following tasks: a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and <u>other data protection provisions</u>; (…)

b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;	b) to monitor the implementation and application of <u>this Regulation and of other data protection provisions and of</u> the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits; <u>monitoring shall also cover personal data subject to professional secrecy or special official secrecy.</u>
c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	(…)
d) to ensure that the documentation referred to in Article 28 is maintained;	(…)

e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	(…)
f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;	(…)
g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	c) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating with the supervisory authority at the latter's request; (…)

h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.	d) to act as the contact point for the supervisory authority on issues related to the processing and, in case of doubt, consult with the supervisory authority on his/her own initiative.
2. 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 tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.	(…)

11. **re Article 38: See the note from Germany dated 13 February 2013**

12. re Article 39:

Article 39 ***Certification***	*Article 39* ***Certification***
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	1. With a view to enhancing data protection and the security of processing the Member States (…), the Commission and the supervisory authorities shall encourage, in particular at European level, the establishment of data protection procedures for the elaboration, implementation and development of data protection policies as well as the checking and confirmation thereof by means of awarding (…) data protection seals and marks for procedures and products allowing data subjects to quickly assess the level of data protection provided by producers, controllers and processors. The data protection procedures should be voluntary and transparent and carried out at regular intervals by expert bodies that have no conflicts of interest, and contribute to the proper application of this Regulation and other data protection provisions, taking account of the specific features of the various sectors and different processing operations[1] .

[1] Possible forms that the legal consequences of such checks and confirmation might take are either having due regard to them when fixing the amount of the fine provided for in Article 79(2), or an additional step in the procedure to remedy non-compliance before the imposition of a sanction, similarly to Article 79(3). An additional possibility would be to exempt certified procedures from prior consultation pursuant to Article 34(2).

2.	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 the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	(…)
3.	The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognise certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	(…)

SPAIN

This document is part of our national position on the draft regulation. In order to be consistent, we drafted our latest proposals in track change mode and in the context of our original comments on Chapter IV. Most of those comments are still valid and valuable in order to get a general assessment of this part of the instrument.

Therefore, please maintain document in track changes mode in order to allow easily finding our latest amendments.

Introduction

Chapter IV: Controller and processor

General considerations

Chapter IV contains 5 sections and 18 articles (articles 22 to 39).

This Chapter deals with the regulation of the active subjects of the processing operations: the controller and the processor. Nevertheless, and in line with the regulation of the obligations of each subject, it introduces important dispositions regarding security, such as: impact assessment, prior consultations, communication of incidents, codes of conduct and certifications.

On the other hand, it regulates the figure of the data protection officer, establishing its juridical statute, its rights and obligations.

In sum, it is an important Chapter for the adequate comprehension of the whole system, in which aspects that concern the two fundamental axes of our position are highlighted: the need to find alternatives to certain administrative or bureaucratic burdens, and the double approach on public and private sectors.

Commentaries on article 22

As we will clarify throughout the study of the articles of this Chapter, our position suggests a substantial change of orientation of some of its aspects.

Somehow, there is a need to reduce a part of the administrative or bureaucratic burdens that the actual system imposes to the subjects of the processing operations, but at the same time, to search for elements of flexibility. All of these, on the basis of the paradigm that it might be more efficient to favour organizational autonomy and accountability, than trying to "ensure" results through a control based on bureaucratic and intensive supervision of the actors.

Thus, with the system we propose the higher or lower level of bureaucratic burdens will depend on the decisions of the actors, on the basis of certain and clear rules about the goals.

These options basically consist of:

- To incorporate elements of added value to the organizations, that clearly boosts its level of reliability: the data protection officer, or sound certification policies. In exchange, the organization obtains a relaxation of the bureaucratic burdens and flexibility on the procedures.
- Not to incorporate such elements. In this case, the bureaucratic burdens are increased as the only possible way of supervision.

Bearing this in mind, we propose some amendments on this and other articles of Chapter IV.

In the case of article 22, the amendments proposed are aimed at adapting this regulation to the abovementioned philosophy and to leave without effects the faculty for adopting delegated acts by the Commission in the way expressed by the third paragraph, which disappears, as we consider that it exceeds the legal boundaries. We do not believe necessary to specify other measures, which should be included in other parts of the Regulation, or dealt with by the legislator.

In relation to part 3 of the article, we have underlined it, as we consider that the issue of internal or external audits should be thoroughly examined, so as to clearly define in which cases they are necessary. To begin with, we have amended the paragraph with a reference to the risk levels, because we believe that it is one of the main criteria to take into account.

On the basis of what precedes, these are the Spanish amendments to the article 22:

Article 22

Responsibility of the controller

1. The controller **may** ~~shall~~ adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1, **in the cases referred to and according to the rules established in this chapter**, shall ~~in particular~~ include:

   (a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1), **or obtaining and keeping a certificate pursuant to certificate policies defined by the Commission.**

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized enterprises.~~

Alternatively, we could accept the Presidency's proposal (risk approach document), putting into brackets the reference to the impact assessment.

Commentaries on article 23

In this article, we attend to some of the demands that have been raised by some of the actors consulted, in the sense that the data protection by design should be conceived in a flexible way, attending to each sector's peculiarity.

We draw attention to the circumstance that the breach of this rule shall be sanctioned, and to the difficulties that could arise from the prospective of sanctions typification in order to avoid legal uncertainty.

Nevertheless, we believe that paragraph 2 should be reconsidered from a more genuine privacy-by-default conception. That is why we keep it underlined.

In relation to the delegated acts envisaged in paragraph 3, we consider that they are unnecessary, and thus, they should disappear from the text. Our viewpoint is based on the general approach of the principle of accountability that we maintain in our position document, which will lead the authorities to focus majorly on the objectives and results, rather than on the means. In its case, what is envisaged in this article might be achieved by compilations of good practices that could be provided to the actors, being therefore unnecessary a strictly normative approach.

Article 23

Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement technical and organisational measures and procedures **appropriate to its activity and aim**, in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed, **in a non excessive amount,** ~~which are necessary~~ for each specific purpose of the processing and are especially not collected or retained beyond the **proportionate** minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~

~~4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Alternatively we could accept the Presidency's proposal (risk approach document), as a basis for further discussion:

Commentaries to article 24

We believe that in this article, it is perfectly possible to establish two different models, in a flexible approach, that will allow the actors of the processing to choose between the two of them.

On one hand, the model of solidarity will allow the actor exercise all of his rights against any other actor, corresponding to each actor of the processing operation the burden to ensure the fulfilment of their obligations.

On the other hand, the distribution model, as envisaged in the article. Nevertheless, for this model to affect the actors, it is necessary that they know clearly and precisely before whom should they exercise each of their rights. That will necessarily mean a series of obligations of documentation and transparency of the agreements.

We also understand that this article covers only and exclusively everything related to the exercise of rights by the actors, but not the substantive and judicial actions of patrimonial responsibility produced by harms, which are envisaged in article 77.

Thus, we propose these amendments:

Article 24

Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. **For this arrangement to be presented to the data subjects, it shall be documented and it must have been communicated to them in advance. Otherwise, the aforementioned rights may be entirely exercised before any of the joint controllers.**

Commentaries on article 25

In relation to this article, we believe that the Commission has made an enormous effort to find a compromised solution, in a matter in which it is not easy, due to its own characteristics.

We basically agree with the approach of the article, although we propose to include risk criteria in part b) of the second paragraph.

The article would stay as follows:

Article 25

Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

   (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

   (b) an enterprise employing fewer than 250 persons, **unless the processings undertaken by them are considered as high risk processings by supervisory authorities, according to their characteristics, kind of data or number of data subjects;** or

   (c) a public authority or body; or

   (d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Commentaries on article 26

From our prospective, this article adequately regulates the figure of the processor, although we must introduce three clarifications:

- Paragraph 3 seems excessively bureaucratic. The fact that it is compulsory to document in writing each and every instruction might become a disproportionate burden, especially if it includes the instructions produced once the contract is signed and the ones produced in the context of a contract. Bear in mind that in certain sectors, the instructions might be produced each day, and in high amounts. Anyhow, normally the operative instructions will be sent by electronic means, so there will always be possible to track, and finally, this is an issue that basically affects to the relation between the controller and the processor, but not necessarily to security and privacy. At last, it seems reasonable that the contractual relation between the processor and the controller is documented in any storage system that can be tracked, a wording which we believe is more appropriate than the mere obligation of a written documentation (because it is much more limited).
- As regards to paragraph 4, it seems that in certain cases there might be a coincidence of responsibilities that should be mentioned. Indeed, without prejudice that exceeding powers (ultra vires) could lead to a personal obligation of the processor, we cannot rule out the possible existence of cases in which exists "culpa in vigilando" of the principal (controller).
- The attributions granted to the Commission in this article seem to be excessive. Their content, if it is considered indispensable, should be developed in the Regulation's text.

On these bases, we propose the following amendments:

Article 26

Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. **Wehre the processor is not part of the same group of undertakings as the controller, t**he carrying out of processing by a processor shall be governed by a contract or other legal act, **which shall be documented in a format that shows evidence,** binding the processor to the controller, and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) **determie the conditions to enlist other processors.**

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller **as far as it is possible** in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) **(…) not process the personal data <u>further after the completion[1] of the processing specified in the contract or other legal act, unless there is a requirement to store the data[2] under Union or Member State law to which the processor is subject</u>;**

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

---

1 SI queried when processing was 'ended'.
2 Further to NL and SE suggestion.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24, **without prejudice to the possible liability of the controller with regard to his obligations.**

5. ~~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 the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.~~

Commentaries on article 27

We have nothing to object in relation to this article, although its actual wording does not add practically anything new.

Attending to the explanations of the Commission, it seems like what this article intends to envisage is a definition of the obligation of confidentiality of each person (v. gr. the employees of the company) that by any reason have contact with the processed data. If it is like this, there is no doubt that the actual wording can be improved.

Deletion is suggested

~~*Article 27*~~

~~***Processing under the authority of the controller and processor***~~

~~The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.~~

Commentaries on article 28

This article lays down with great detail the documentation that must be produced by the subjects that take part in the processing operations of the personal data.

Somehow, this article constitutes a sort of counterbalance for not demanding a previous authorization for data protection.

From our point of view, the article introduces an excessive level of administrative burdens.

It should be taken into account that those companies that have appointed a Data Protection Officer have already such a level added value in terms of trust and security that it would not be risky to reduce the administrative burdens, and to open new paths based on accountability.

Somehow, the additional cost and effort derived from the incorporation of a Data Protection Officer to the organization, provided with a statute that grants a relative independence, linked to the staff and equipment required, must be compensated with the establishment of flexibility criteria for the management of the company and to discipline its accountability.

The abovementioned must also be applied to organizations that have established strict certification policies. These policies, to which we will refer to in article 39, must be in disposition to offer a level of high consciousness and quality, so that may be a reasonable alternative to the Data Protection Officer (which means higher costs) without renouncing to high levels of reliability.

At last, what concerns the data and privacy protection is that the organization that will process the data is reliable and that it is always able to account for effectively, so it is not necessary to establish formalities that exceed the boundaries of the pretended goal, and that impose unnecessary costs, burdens of management or simply limits to the power of organizing, if this objective can be fulfilled by supervision when it is necessary.

Consequently, we believe the paragraph 1 of this article should just word a clear and universal principle of accountability: the controller of the processing operations should always be able to inform the authorities that require so of the operations under their responsibility.

No-one, small though they might be, must be out of the reach of this principle. Obviously, the level of detail, formalism and precision for the accountability should be reasonably modulated depending on the dimensions of the organization, the level of risk of their activities or the confidentiality of the processing operation.

From that point, each organization, if they have a Data Protection Officer, or a certification policy which is sufficient and in force, must be granted with organizational flexibility, with the only compromise of the result pursued by the Regulation; that is to say: being able to inform adequately. Whether this is fulfilled by pre-existing documents or by electronic reports, is secondary if in the end it is possible to supervise when it is necessary.

Note that we are not defending here that the existence of a Data Protection Officer or a certification policy exonerates from the obligation of documenting or being able to inform of the processing operations developed. What we are saying is that when an organization is provided with these elements of added value, the means of doing so rests in hands of the controller, which is subjected to the obligation of being able to inform in any time of each and every aspect of their processing operations.

On the contrary, for those organizations with more than 250 workers that have not named a Data Protection Officer or a certification policy, it does seem necessary to establish rigid criteria of accountability: to produce a minimum of documentation with the required formalities envisaged in the law. Somehow, the non-existence of the Officer or the certification policy, linked to the dimension of the organization, generates a risk that has to be attended to by the legislator.

This leaves us to deal with the situation of the organizations with less than 250 workers that have no Data Protection Officer.

It is clear that for the small and medium organizations, the Data Protection Officer will normally be too expensive, so it will not be possible to name one in most cases. As for the certification policies, although recommendable from a wilfulness point of view, might be excessive if they are directly imposed, attending to the low level of risk.

For such situations, paragraph 4 of this article excludes the requirement of the documentation envisaged in the second paragraph, except for the organizations that are specifically to the activity of processing of personal data. These organizations may choose between the three options: officer, certification, or the documentation required by the law.

According to our amendments, it is not excluded on the contrary, the general principle of accountability, as it has been worded in the first part of the article. We understand that it would not be viable for a democratic society not to regulate such a principle, even though the accountability must adapt to the dimensions of the organization and the risk of its activity.

Dealing now with the bureaucratic requirements contained in the article, we understand that, in coherence with the abovementioned approach of the Spanish position, the time limits for erasure of the different categories of data envisaged in art. 28. 2. g) should operate with certain flexibility, because in many cases it is very difficult to know this particular point in advance, or to fix it with precision.

On the basis of the abovementioned, the article, once amended, remains as follows:

Article 28

Documentation

1. Each controller and processor and, if any, the controller's representative, **shall be in a position to adequately inform the authorities that request it on** ~~shall maintain documentation of~~ all processing operations under its **own** responsibility.

2. **The enterprises or organizations that do not have a data protection officer or sufficient certificate in force, shall have the legally established documentacion form with regard to all processing operations carried out under their resposibility.** ~~The~~ **This** documentation shall contain at least the following information:

   (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

   (b) ~~the name and contact details of the data protection officer, if any;~~

   (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

   (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

   (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

   (g) **where possible,** a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available **concerning operations under its own responsability**, on request, to the supervisory authority.

4. The obligations referred to in paragraph~~s 1 and~~ 2 shall not apply to the following controllers and processors:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. 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 the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission ~~may~~ **shall** lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Commentaries on article 29:

In relation to this article, it is necessary to point out that in most cases, it is the controller, and not the processor, who will keep in relation with the supervisory authority, although the processor may be sometimes required by the authority.

This is why we think it is necessary to clarify the first paragraph so that the processor shall only account where appropriate, but not in general, like the controller.
We also miss a reference in paragraph 2 to the representative for the cases in which the responsible are beyond the EU boundaries.

Finally, we suggest studying the possibility of moving the content of this article to article 53, for a better systemization of the Regulation. This is why we underline art. 29**, and will not be against deletion**.

Therefore, we propose the following amendments:

Article 29

Cooperation with the supervisory authority

1. The controller and the processor **where appropriate** and, if any, the representative of the controller, shall cooperate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller, **himself or through his representative,** and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Commentaries on article 30:

In our view, in security matter it is enough to determine the objectives clearly, and that, from there, the results are supervised and the necessary corrective measures are taken.

So, it is necessary to open spaces of flexibility so that the actors can establish security measures, attending to the peculiarities of each sector, without being necessary to regulate in detail through delegated acts.

We propose to amend the text as follows:

Article 30

Security <u>and confidentiality</u> of processing

1. **<u>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 fundamental rights and freedoms of data subjects,</u>** the controller and the processor, in each respective leves, shall implement appropriate technical and organisational measures**<u>, including the use of pseudonymous data,</u>** to ensure a level of <u>confidentiality and</u> security appropriate to the<u>se</u> risks (…).

2. (…).

2a. **<u>The obligation of confidentiality on any person acting under the authority of the controller or the processor shall continue to have effect after the termination of their activity for the controller or processor</u>**

~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.~~

~~4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:~~

~~(a) prevent any unauthorised access to personal data;~~

~~(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;~~

~~(c) ensure the verification of the lawfulness of processing operations.~~

~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Commentaries on article 31:

In our view, this article is excessively bureaucratic, and seems to focus on the documentation of the problems, rather than on an agile and efficient solution.

Thus, we understand that it is convenient to modify this norm, on the basis of the following criteria:

- It does not seem reasonable to impose the notification and documentation of any security breach, but only of those that, because of their characteristics, will imply a significant risk for the privacy. An excess of notifications, including minor breaches without further consequences might end up reducing the capacity of control and the concentration of the supervisory authority.
- The period of 24 hours established in the first paragraph may not be possible to achieve in many cases. We think it is fundamental to establish criteria of reasonable shortness, so it is preferable to include the wording “undue delay”. All in all, we do not rule out a solution such as the one proposed by the DAPIX Group for article 29: a two-phase notification (immediate or without delay warning of the existence of a problem and the subsequent notification with further details in a wider –but limited- period).
- We do not think either that it is necessary to regulate in detail the content of the notification, due to the peculiarities of the different sectors. In our view, it should be enough to communicate what the supervisory authority really needs to correctly estimate the incident and its consequences. To this effect, the fundamental elements of the act of communication should be: the facts, the proven/envisaged consequences, the measures adopted or/and to adopt.
- Certainly, there might be minor incidents related to security, that though they are not a direct risk for privacy, it is convenient to detect and register them, so that they can be prevented in the future. To this effect, we believe it would be advisable to keep a record of minor incidences related to data protection accessible to supervisory authorities.

- At last, the delegated acts conferred to the Commission should be limited to those required for establishing a unified format of the notification of incidents and for the registry of breaches and incidences.

On this basis, we propose the following amendments:

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach **that because of its characteristics represents a significant risk for people's privacy**, the controller shall without undue delay ~~and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.~~

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach **described in paragraph 1.**

3. The notification **must have the necessary elements for the supervisory authority to assess the facts and their consequences and, where appropriate, remedial action to be taken.** ~~referred to in paragraph 1 must at least~~:

~~(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;~~

~~(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;~~

~~(c) recommend measures to mitigate the possible adverse effects of the personal data breach;~~

~~(d) describe the consequences of the personal data breach;~~

~~(e) describe the measures proposed or taken by the controller to address the personal data breach.~~

4. The controller shall document any personal data breaches **as referred to in paragraph 1**, comprising the facts surrounding the breach, its effects and the remedial action taken. **Without prejudice to the latter, the controller or, where appropriate, the processor shall operate a register of errors and incidents not referred to in paragraph 1 but with a relation to personal data processing, available for the supervisory authorities which may ask for a copy of it to be sent to them periodically.** ~~This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.~~

~~5. 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 establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.~~

6. The Commission may lay down the standard format of ~~such~~ notification**s** to the supervisory authority, **in the terms established in paragraph 3, as well as the register of errors and incidents** ~~the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein~~. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Commentaries on article 32:

In general we agree with the wording of this article. More specifically, we believe that the wording of the first paragraph is correct, and the way in which the notification to the actors through the combination of this paragraph with paragraph 3 is enclosed.

<u>All in all, we think it is necessary to envisage some kind of safeguard for those cases in which the notification to the actor, or to some of the actors, may be harmful to an investigation and/or a resolution of the breach o security. To this effect, we propose to include a new paragraph, after the fourth, which establishes these exceptions.</u>

Agile procedures for the notification for those cases in which the number of affected actors is high are also needed, and for this, we think it is convenient to empower the Commission to develop the works in the frame of the principles and limits envisaged in this article.

At last, the actual paragraph 5 must be erased, because the powers granted to the Commission exceed the nature of delegated acts. The correct interpretation of the cases envisaged in art. 32 should be developed by the system of supervision and the courts, not by the Commission.

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach ~~and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).~~

3. Notwithstanding paragraph (1), the communication of a personal data breach to the data subject shall not be required if the controller (…) has implemented appropriate technological protection measures and **(…)** those measures were applied to the data **affected by** the personal data breach. Such technological protection measures shall **include those that** render the data unintelligible to any person who is not authorised to access it**, such as encryption or the use of pseudonymous data**.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

The data subject shall not be communicated in the cases where this communication may clearly hinder ongoing investigations or hinder or delay the solution to the breach of security. Member States may develop these cases trying to meet a public interest objective and respecting the core content of the right to the protection of data[1]**.**

5. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.~~

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication, **specially taking into consideration the cases with a high number of concerned people**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Commentaries on article 33:

This norm envisages the need to develop impact assessments when the projected processing operation might produce specific risks for the rights and freedoms of individuals.

The main objective of these assessments is to prevent, because in those cases in which there is a high risk, the processing operation is subjected to a prior consultation with the supervisory authority (art. 34. a)

[1] Another alternative could be following the wording of the Article 3(5) of the **Draft Commission Regulation on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications: "***In exceptional circumstances, where the notification to the subscriber or individual may put at risk the proper investigation of the personal data breach, the provider shall be permitted, after having obtained the agreement of the competent national authority, to delay the notification to the subscriber or individual until such time as the competent national authority deems it possible to notify the personal data breach in accordance with this Article."*

In our point of view, this article introduces an important factor of bureaucratization to the whole management of processing operations, especially taking into account that a part of the actors might be compelled to develop this type of assessment are organizations that will have a Data Protection Officer.

Certainly, there might be small organizations that, because of their activity, require to process high risk personal data, but for these cases, less burdensome but effective solutions could be found, like the system of certifications, especially conceived for high risk processing operations, as envisaged in art. 39.

On the other hand, the cases described in paragraph 2 are excessively generic and abstract, so we consider that they should be revised: the impact assessment should only remain for those cases in which there is a true risk that can not be prevented by less burdensome means.

Paragraph 4 should be also reconsidered, due to the difficulties and important costs that the opinion studies might bring.

In what paragraph 6 is concerned, we believe that the delegated acts are not justified in this case, because they would develop essential aspects of the Regulation. In our viewpoint, it is the propper Regulation which has to determine ots own scope.

Thus, we propose this new wording of the article:

Article 33

Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, **in the cases where the organization has no data protection officer or sufficient certificate in force for processing high risk data.**

ES believes that DAPIX should continue working on art. 33.2, trying to find a more balanced approach based on juridical certainty and trying to avoid excessive burden.

Meanwhile, we do think that the presidency's proposal is better than the Commission's draft:

2. The following processing operations (…) present specific risks referred to in paragraph 1:

(a) a systematic and extensive evaluation **on a large scale** of personal aspects relating to **(…)** natural person**s (…)**, which is based on automated processing and on which decisions[1] are based that produce legal effects concerning **(…) data subjects** or significantly affect **data subjects**.

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

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale[2];

(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 fundamental rights and freedoms of data subjects**[3].

---

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 BE and FR 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',

3 BE suggested deleting this subparagraph.

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. [1]

2b. Prior to the adoption of the list the 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 in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union. [2]

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the 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 the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law **or the law of the Member State to which controller is subject**, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

---

1 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2.

2 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2.

6. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Commentaries on article 34:

Again we find in article 34 a norm thought to increase the security of the processing operations that intends to achieve its objective by introducing a series of bureucratic burdens, which could be avoided by alternative means.

Indeed, for those organizations that have a Data Protection Officer it seems necessary to establish compensatory measures to the administrative burdens, beacause the officer generates such an extra of security that it should allow us to relax the security measures based on administrative control.

And, because it is not possible for every organization to name an officer with the team and technology required, it is also necessary to search for alternative instruments to avoid that the overburdening falls only on those organizations with fewer resources. Again, for us the alternative should come from the application of mechanisms of accountability, such as the certifications envisaged in article 39.

Without prejudice of the abovementioned, the article should be subjet to thorough reconsideration. The problems faced on paragraph 1 should be solved in the regulation of the international data transfers, and paragraph 2.b) seems rather uncertain, especially because it may derive in a multiplicity of criteria against, precisely, the desireble principle of uniformity, which can also be argued about paragraph 4.

In relation to paragraph 7, although it seems positive that consultations in order to ensure the quality and suitability of the legislative processes are established, we do not believe that a Regulation of the EU is the most appropriate instrument to envisage laws of this type that affect the legislative procedure of the Member States.

On the other hand, there is nothing to object against the delegated acts in this case.

We propose to amend the article as follows:

Article 34

Prior authorisation and prior consultation

1. The controller or the processor as the case may be, **in the cases where the organization has no data protection officer or sufficient certificate in force,** shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf, **in the cases where the organization has no data protection officer or sufficient certificate in force,** shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

   (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

   (b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. ~~Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.~~

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.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Alternatively, ES could accept the text proposed by the Presidency (risk assessment document), but only if the need for prior authorisation applies when there is no DPO appointed or no certification covering those circumstances has been issued and remains in force.

Commentaries in article 35:

In our point of view, the figure of the Data Protection Officer might become of great importance for the correct implementation of the Regulation.

The best way to implement this figure is not to oblige, but to encourage and to rise awareness.

This is why we believe that the officer should be voluntary, not compulsory, and that it should be promoted by conferring certain benefits such as the relaxation of bureaucratic burdens and the flexibilization of procedures and processing operations. Furthermore, we understand that there is nothing against the Member States adopting in their public policies other incentives that supplement the ones envisaged in this Regulation.

Indeed, the existence of an officer in an organization, provided with the capacities required by its role, including the personal and material resources, and acting with a propper juridical statute, constitutes an extremely valuable guarrantee for the Regulation's success, and for the privacy protection.

Furthermore, although it is true that the officer should develop his role under premises criteria of strict proffesionality (amendment to paragraph 5), one of the reasons why the Data Protection Officer should be dismissed is the serious lack of attention of those criteria (amndment to paragraph 7).

Form the wording of article it can be deduced that the officer may be subject to different juridical statutes. In this sense, it can be designated among the staff members of the organization (administrative or labour regime), or it can be an independent service provider, both a physical and a juridical person (service contract). Thus, we believe that the normative development lacks of specific dispositions established for those cases in which the relation is externalised through service contracts, because it is a different case than the administrative or labour vinculation.

An example of what we are saying is paragraph 7, which establishes, as a safguard, a minimum period during which the officer can not be dismissed if it is not because of disqualification or non-compliances. This safeguard may collide with the freedom of service contracting, and even affect negatively the competence in the market. Furthermore, if the officer is already a member of the staff of the organization, this same time limitation might have impact on several aspects of labour law or statutory civil servant law as well.

Because of these, we believe that the safeguards and guarrantees of the officer can be obtained by other means, avoiding the time limitation of article 35.7.

As for paragraph 10, we have doubts whether it is necessary to communicate publicly the name of the Data Protection Officer. This does not add value to the protection of privacy, and at the same time, it requires the unnecessary processing operation of a personal data. In our view, it should be enough to refer to the users, clients and other actors, ant to indicate that what they will be communicated, if it is the case is the contact information of the officer.

And we say “if it is case” because, in relation to paragraph 10, we have doubts whether it is adequate to establish this sort of right of direct contact with the officer, for that would have an impact on the organizational faculties of the corporation. What it should be dealt with in this article is something that affects directly to the true nature of this juridical figure: to determine whether the officer is a consultant of the organization, or a defender of the rights of the clients. Additionally, in same cases (police, security servicis, and similar) it may not be advisable to give full identification of the individuals that act as DPO’s.

On the other hand, and on the basis of the new propossed approach, we understand that the delegated acts envisaged in the article are not necessary. Indeed, the letters a) to c) have been deleted in our position, and the requirements or profesional profile of the Data Protection Officer should not be regulated in a normative act; it is something that should be left to the criteria of the different actors, depending on their needs and according to their goals, obviously without prejudice that orientative or good practices standards could be established.

This is why we propose to amend article 35 as follows:

Article 35

Designation of the data protection officer

1. The controller and the processor ~~shall~~ **may** designate a data protection officer ~~in any case where:~~

   ~~(a) the processing is carried out by a public authority or body; or~~

   ~~(b) the processing is carried out by an enterprise employing 250 persons or more; or~~

   ~~(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.~~

2. ~~In the case referred to in point (b) of paragraph 1, a~~ **A** group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several **(…)** such authorities or bodies, taking account of their organisational structure and size.

4. ~~In cases other than those referred to in paragraph 1, t~~**T**he controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37**, under the strict criteria of professionalism**. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. ~~The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms.~~ During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties**, or if there is a serious non-compliance related to these duties.**

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation. To that end enough contact details shall be given by the controller or the processor.

~~11. 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 the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.~~

Commentaries on Article 36:

The second paragraph of article 36 lays out an issue of utmost importance for the correct delimitation of the figure of the Data Protection Officer. Indeed, this paragraph regulates that the "controller or the processor shall ensure that the data protection officer performs the duties and tasks independently".

This idea of independence is an undefined concept without a precise scope, although it can be easily related to the idea of independence attributed to the supervisory authority.

Nevertheless, it does not seem like that comparison can be made automatically. Indeed, the officer is, firstly, a person linked to the organization, and works for it. It is, therefore, subjected to its hierarchy and organizational powers, and its task is to contribute to achieve certain goals, both public and/or private.

Thus, it is necessary to determine how the principle of independence is compatible with the position of the officer in the organization.

In our view, the answer to this question requires to understand that the officer is subjected to, on one hand, the institutional discipline, but on the other, it has a legal order to act objectively and according to the principles and procedures envisaged in this Regulation. But this does not mean that its behavior can be completely exempt or even act against the objectives of the organization.

Therefore, we recommend not to use here the concept of independence, but to resort to an alternative wording, which is much more descriptive and adjusted to the reality of the figure of the officer.

The new wording could be: “The controller or processor shall ensure that the data protection officer performs the duties and tasks in accordance with the present Regulation and does not receive any instructions as regards the exercise of the function”.

As for the third paragraph, it seems as it has been worded bearing onlyin mind the situations in which the officer is related to the organization by statutary or a labour contract with the organization, because the wording does not match with the externalization by the service contract option. Therefore, it should be modified as follows: “The controller or the processor shall support the data protection officer in performing the tasks and, when necessary, shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37”.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer **performs the duties and tasks in accordance with the present Regulation.**~~is properly and in a timely manner involved in all issues which relate to the protection of personal data~~.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently **and does not receive any instructions or experiment any actions or omissions that may prevent, obstruct, impede or interfere the due exercise of its functions** The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and**, when necessary,** shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

4. The data protection officer may fulfill other tasks and duties. The controller shall ensure that any such tasks and duties do not result in a conflict of interests[1].

Commentaries on article 37:

In accordance with the amendments to article 35, for the Regulation to be coherent article 37 should be modified too.

We are also doubtful about the obligatory nature of the direct relation with the supervisory authority of letters g) and h), for this would interfere with the domestic faculties or auto organizational powers of the company.

[1] Moved from Article 35 (6). DE was opposed to this as these requirements were irrelevant to the functional independence of the DPO. UK also thought this was too prescriptive. Presidency endeavoured to redraft this paragraph in order to make it less prescriptive.

On the other hand, we understand that the task of the Commission should focus on the certification and the statute of the officer, so that where this figure exists; the post is occupied by someone who has the required capacities and protected the necessary guarantees.

We therefore propose to amend article 37 like this:

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

   (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation ~~and to document this activity and the responses received~~;

   (b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

   (c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

   ~~(d) to ensure that the documentation referred to in Article 28 is maintained;~~

   (e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

   ~~(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;~~

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating with the supervisory authority at the latter's request or on the data protection officer's own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. 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 ~~tasks,~~ certification, status **of the data protección officer**, ~~powers and resources of the data protection officer referred to in paragraph 1~~.

Commentaries on article 38:

We applaud the introduction of Codes of Conduct by the Commission. It seems an alternative that may become helpful, especially to solve certain problems or doubts we had. The fact that the past experience has not been vey successful should not discourage us to search for new instruments of auto-regulation or co-regulation, because it has been proven that when they work, the sustainability and the level of satisfaction among the actors is higher.

Firstly, it strikes that there is no definition of what should be understood by Code of Conduct. Perhaps we should consider introducing the definition of these codes in article 4.

A very important aspect in relation to these kinds of instruments is the one regarding the participation in their development. Depending on how this development is arranged and how the participating actors are selected, the results might be very different. We believe that we should not reduce the participation to a verification of the adequacy by the supervisory authorities or by the Commission. In this sense, we think that we should search for models that favour a wider participation, so that the most relevant actors may take part. The practice shows that if we do not take this into consideration, problems will be arisen.

However, we should try to find compensations that serve as instruments of encouragement of the Codes of Conduct as well. This is in our view another of the key elements for these instruments to success.

It also worries us the fact that the Codes of Conduct might come to fossilize due to the nearly prescriptive empowerment envisaged in favour of the Commission.

Finally, and as a warning, at the time of exploring the possibilities of these instruments, we should take into serious consideration the risks involved: fundamentally, the collusive behaviours that might harm the technological or competition development.

We propose to word the article as follows:

Article 38

Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the **participatory** drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, and the specific needs of micro, small and medium-sized enterpises, in particular in relation to:

   (a) fair and transparent data processing;

   (b) the collection of data;

   (c) the information of the public and of data subjects;

   (d) requests of data subjects in exercise of their rights;

   (e) information and protection of children;

   (f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

~~4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).~~

~~5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.~~

Commentaries on article 39:

In our view, the certifications may become a fundamental tool to achieve the goals intended by this Regulation.

Indeed, beyond the role that the present proposal envisages for the certifications, we think that they might constitute an effective alternative to ease the management for the different actors and to relax, in exchange for implementing them, some of the administrative burdens and to flexibly some of the procedures.

To achieve this it is necessary that certifications are articulated through a strict procedure for the strengthening of the capacities; a procedure that should also be provided with the required flexibility. With this we are pointing out that the certifications should be subjected to renovation and actualization in certain cases.

Moreover, when serious breaches that contradict their maintenance occur, there should be a possibility of cancelling the certifications. This must lead immediately to the loss of the benefits that they might produce.

Only with these kinds of guarantees the certifications may lead to certain benefits for the organizations that chose this system. That way, it is possible to combine the privacy protection with the necessary management flexibility required by any organization.

We propose the following wording for article 39:

Article 39

Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification **policies** ~~mechanisms~~ and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certification ~~mechanisms~~ **policies** shall contribute to the proper application of this Regulation, **and to obtain the options and benefits derived from it**, taking account of the specific features of the various sectors and different processing operations.

The certification policies at EU level shall be designed by the European Data Protection Board with the participation of other relevant actors, and shall be approved by the Commission. Not only shall these policies focus on the Institutions, but also on operators in this field.

The certification policies shall pay attention to the specific needs of the actors in the different sectors of activity, specially taking into account the requirements of micro, small and medium companies, and the necessary cost containment to make these policies effective. The obtaining, renewal or loss of the certifications will produce the legal consequences provided by this Regulation.

2. 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 the data protection certification mechanisms referred to in paragraph 1, including conditions for granting ~~and,~~ withdrawal~~,~~ **and expiration**, and requirements for recognition within the Union and in third countries.

3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Conclusions:

As we said before, this chapter brings up very relevant issues that affect two axes of our position: administrative burdens and the public-private sector approach.

In general terms, the architecture proposed in what the active subjects are concerned seems adequate and realistic. The dichotomy between processor and controller of the processing operation will allow us to offer a proper response to most of the cases. Nevertheless, the regulation keeping its technological neutrality should give adequate solutions for Cloud Computing environment.

Our amendments to this chapter try to promote an alternative by which there is a substantial decrease of bureaucratic and administrative burdens in exchange for a greater effort of the actors in the area of accountability.

Indeed, the main objective is to provide the system with certain flexibility, opening spaces so that every actor can organize its activities with responsibility, and so that these activities are subjected to a high security paradigms and a sufficient accountability is always ensured.

This is achievable by promoting the figure of the Data Protection Officer and the certification policies.

The figure of the officer may be promoted by encouraging its incorporation to the administrative or corporate model and by strengthening its juridical statute, so that they can develop their tasks with professionalism and independence.

Obviously, we are conscious that the incorporation of this officer to an institutional structure has its costs: the need to employ a highly qualified person, the necessity to provide the personal and material resources… Nevertheless, the possibility of sharing the costs of the officer with other organizations, both in the public and private sector, opens great opportunities.

Even so, our position paper envisages alternatives for those cases, fundamentally in micro, small and medium corporations, in which because of its cost or because of the small amount of data processing operations, it is not realistic to incorporate an officer to their staff.

For these cases, we believe that the certification policy might be an adequate alternative.

We believe that this alternative is a true certification policy, which ensures that what is certificated is always a serious commitment with the protection of privacy through the protection of personal data.

To this effect, the certifications must be titles subjected to continuous revisions and to the caducity derived from the absence of renovation or serious breaches.

This certification policy may be implemented by the Commission with the support of the national supervisory authorities, but always opening channels of participation for the different actors involved.

In exchange for all this, the documentation, impact assessment, prior consultation and breach notification obligations are remarkably relaxed.

This relaxation does not necessarily mean lack of attention to the fact that these measures do have a positive impact on the privacy protection. In other words, what we propose does not mean that there are no documentation obligations at all, or that there is no safeguard of the impact of the processing operations, or for the consequences that the breaches of security might produce. On the contrary, what happens is that more flexible alternatives for all those obligations are offered, on the basis of strengthening the capacities of accountability of the actors.

Finally, and as a general reflection, in what active subjects of the processing operations are concerned, we would suggest avoiding excessively general approaches, which include both the controller and the processor. Both subjects have different roles and objectives, so a common regulation that entails unnecessary duplicities of bureaucratic burdens must be avoided.

FRANCE

France wishes to begin by stressing that **these comments apply to the versions of Articles 28 to 39 in 16529/12, dated 4 December 2012, and do not include comments on the new version presented by the Irish Presidency.**

As to methodology, France will not repeat comments it has already made in Working Party meetings, but notes that it has entered a scrutiny reservation on 5703/12 and that it hopes that future proceedings will allow delegations the time to give the negotiations all the attention they need.

Chapter IV

Section 1 - General obligations

Article 28 - Documentation

In paragraph 1, France wants the documentation requirement, and in particular its scope, to be adjusted (not removed) depending on the level of risk - a concept which should also be at least defined in the Regulation, to avoid any legal uncertainty for the controllers and the data subjects.

In addition, the French authorities have noticed a translation error at the end of the sentence in the French version, and therefore request that "effectués" be replaced by "mis en œuvre".
Finally, the difficulties of translation between the French and the English versions, mentioned with regard to Article 26(3), recur in Article 28(1). The French version reads "*conservent une trace documentaire* " while the English version reads "*shall maintain documentation*". A single wording should be adopted and used throughout the text.

In paragraph 2, the French authorities want the list of documentation that the controller must keep to be exhaustive, and we are therefore completely in favour of deleting "*at least*".

In point (g) in the same paragraph, we would like the word "*general*" deleted, so as to comply with the principle of proportionality. The controller must know, from the point when the processing is being planned, how long it will be necessary to keep the data.

In point (h) in the same paragraph, for the sake of clarity and consistency, the French authorities request that the words "*in Article 22(3)*" be replaced by "*in Article 22(3) and in Articles 23 and 30*". It seems appropriate for the controller to keep documentation, inter alia, on the measures taken pursuant to the principle of "data protection by design" and on the security measures put in place. The obligation to assess risk imposed by Article 30 will have no meaning unless the assessment is documented, since it will not in practice be verifiable.

In paragraph 4, we think all controllers should be required to keep all documents relating to the implementation of the processing, and we support the deletion of (a) and (b).

As regards the new point (c), France would like the documentation requirement to be reintroduced for low-risk processing operations, with a reduction in the requirement based on the level of risk involved in the processing. Adding an exception for such "low-risk" processing would not meet France's requirements, contrary to footnote 409. The risk-based approach should be implemented by laying down more flexible requirements when the data processing operations present little or no risk, but definitely not by completely removing any documentation requirement. Furthermore, criteria other than the type of data gathered (e.g. the purpose of the processing, the number of persons concerned, etc.) should be taken into account to determine whether a processing operation could affect the fundamental rights and freedoms of the data subject. France again stresses the need to define "risky processing".

Finally, France also requests clarification of how long the controller has to keep the documentation.

Article 29 - Cooperation with the supervisory authority

France favours deletion of this Article, in line with its request in the DAPIX discussions.

Section 2 - Data security

Article 30 - Security and confidentiality of processing

We wish to begin by stressing that in France, the practical implementation of measures to ensure the security of processing draws on the preliminary discussions held at the time when the initial set-up of the processing is declared to the data protection authority.
As things now stand, we have questions about how security measures and risk assessment are defined. We would therefore like clarification on these points and on the possible involvement of the European Network and Information Security Agency in defining the criteria and requirements for the technical measures to be implemented.

France would also like further clarification about the change of title and the addition of "confidentiality"; this notion is in principle included in that of "security" of processing, along with identification, authentication and integrity. We therefore have a scrutiny reservation, pending discussions about the risk-based approach.

Re paragraph 1, we reiterate that that we would like to know what risks it concerns: risks linked intrinsically to the processing, or risks for the data subjects? It seems necessary here to discuss the concept of "risks" before examining the changes proposed in specific articles, which all propose adding this term without its being defined.

On this point, the French authorities stress that they believe it necessary to distinguish risk assessment by the controller, which must concern data processing security, which is the subject of this article, from the assessment of risks for data subjects, i.e. the harm they could be subject to (identity theft, physical harm, damage to reputation, etc.).

In any event, since this Article formulates a requirement regarding outcomes, the French term "garantir" should be replaced by the verb "assurer". In addition, this requirement regarding outcomes seems incompatible with the constraints which are then imposed as regards technical developments and the costs of their implementation.

We note the proposal to delete paragraph 2. However, the additions to paragraph 1 do not meet our concerns regarding paragraph 2 in the initial version.
We therefore reiterate that we would like clarifications on what precisely is covered by the concept of "*evaluation of the risks*".
Should this evaluation of the risks be considered compulsory before any data processing, which - depending on the requirements for this risk evaluation, which will be laid down, as the text stands, by delegated acts - could prove a burdensome obligation for the controller or the processor? If so, one alternative would be to make this assessment compulsory only for the most sensitive data-processing operations. This assumes clarification of that idea.

We are also pleased that account has been taken of our comments on the relationship between paragraph 2 of this Article, in particular the words "*accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data*" and point 9 in Article 4, which defines "*personal data breach*", and which refers to "*accidental or unlawful destruction, loss*" in different terms. We therefore welcome the proposed use at the end of the first paragraph of a single term, namely "*personal data breaches*", defined in point 9 of Article 4, which furthermore covers the cases mentioned in a more general way.

Still on the old paragraph 2, given that this request has not been taken into account in the amended first paragraph, nor elsewhere in the Article, we also stress that this risk evaluation should be linked with the impact analysis in Article 33. Should we take it that the risk evaluation precedes the impact analysis? Could the risk evaluation and the impact assessment be one and the same thing? We think this should be clarified.

On paragraphs 3 and 4, we refer to our general comment on the use of delegated and implementing acts.

Article 31 - Notification of a personal data breach to the supervisory authority

First, we stress that this Article should be checked for consistency with the existing texts (Directive 2002/58 on ePrivacy) and those currently being negotiated (draft Commission Decision on notification of personal data breaches).

In general, we refer back to our earlier comments to the effect that this Article imposes new constraints on enterprises which do not seem readily compatible with the aim of simplifying and reducing the burdens imposed on them. We therefore support the restriction of cases where the controller has to notify a data breach to the supervisory authority introduced in this article and the taking into account in paragraph 3 of the principles of necessity and proportionality of the data processed.

Re paragraph 1, we would emphasise that under the "telecom package", the draft Commission decision currently being negotiated allows a period of 24 hours to inform the supervisory authority that there has been a data breach and four days to inform the affected parties. We would like these two distinct deadlines for notification to be adopted in the proposal for a Regulation, which would allow for more detailed information to be provided by the second deadline. Furthermore, in view of

the submission of a draft text by the services of DG CONNECT under the committee procedure, on Directive 2008/58 on ePrivacy, the purpose of which is to make notifications of security breaches subject to a 24-hour deadline regardless of how serious the breaches are, we would like to see better coordination between the Commission services, so that discussions on the proposal for a Regulation are not held up by parallel proceedings in other Commission services.

We also urge that notification should be restricted to cases of risk to the data subjects. However, this concept needs to be clarified.

On paragraph 2, we have the same remark as on Article 26(2): the processor's obligation to contact the supervisory authority should be removed, and it should be able to contact that authority only through the controller.

On paragraph 3(d): the obligation to describe the consequences of data breaches should also be formulated in a more realistic way, and the words "*identified by the controller*" should therefore be added to the sentence.

Regarding point (f) in the same paragraph, we favour the addition of "where appropriate", which would meet the request expressed during discussion of this Article, and allow the controller's obligations to be reduced.

Article 32 - Communication of a personal data breach to the data subject

In general, we stress again that this Article imposes new constraints on enterprises, which do not seem readily compatible with the aim of simplifying and reducing the burdens imposed on them. We hope therefore that the communication requirement in this Article can be framed more realistically, taking into account the principles of necessity and proportionality. What about

archives? This Article should not require them to seek the data subject to notify him or her of the breach, given that they did not carry out the initial data collection.

As regards paragraph 1, we hope there will be express provision for cases where the victim data subjects' contact details have been lost. We would also like clarification of the nature of security breaches that significantly affect the individual. This criterion, which would be the same as for Article 31, should be clarified.
Lastly, we ask for a restriction to be added to cover the case where such communication would adversely affect an overriding public interest. In some cases it may be necessary not to disclose such information to the data subjects. The possibility of a derogation by national law under Article 21 of the Regulation is not sufficient, and a public-sector derogation should be provided directly in Article 32.
We therefore ask for the following addition to the sentence: "*provided that such communication does not adversely affect a clear public interest."*

In paragraph 3, we would like clarification, inter alia as regards the application of this paragraph to archives and on the concept of "*communication […] to the data subject*" and the differences between that communication and "*information to the data subject*". If the two terms are synonymous, a single term should be used.

In the same paragraph, we think that "*to the satisfaction of the supervisory authority*" introduces a subjective notion that should not appear in legislation.

Finally, we would like clarification of why the mere demonstration that technological measures have been used should lift the requirement to communicate a breach to the data subject. We also wonder about the link between this dispensation and the communication requirement laid down in paragraph 1. It seems preferable to notify only the supervisory authority of the breach, leaving it for the latter to notify or arrange for notification of the data subject.

Section 3 - Data protection impact assessment and prior authorisation

Article 33 - Data protection impact assessment

In general, we stress again that this Article imposes new constraints on enterprises, which do not seem readily compatible with the aim of simplifying and reducing the burdens imposed on them. While assessing the risks associated with a processing operation is a fairly standard procedure, in contrast, the potential risks to data subjects often seem "unlimited", in particular in the case of open processing operations across networks. The controller here therefore faces a greater burden of requirements imposed, and in a position of legal uncertainty, even though it should not be the controller's task to analyse and assess all the risks that could arise through the use of data by third parties.
The requirement to carry out impact analyses should in particular be framed more realistically, taking account of the principles of necessity and proportionality and a criterion based on how critical the data are. A definition of the concept of risk, which is only mentioned in the Article, is needed to give certainty to the situation of controllers and data subjects.

Also in general, we wonder about the application of this Article to personal data processing for historical or scientific purposes, since for archives, the data were originally collected for other reasons.

Finally, we wonder about the relationship between this Article and Article 34. Taking these Articles together, as they stand, the distribution of tasks between controller, processor and data protection authority cannot be understood.

On paragraph 1, we think that again the concept of processing operations which present "specific risks" needs to be defined in the body of the Regulation, not by a delegated act, as currently provided for by paragraph 6.

On paragraph 2, for the reasons indicated above concerning paragraph 1, we welcome the removal of the words "in particular", with the consequence that the list of processing operations in this Article is henceforth exhaustive.

However, in the same paragraph, in paragraphs (a), (b) (c) and (d), the concept of "large scale" should be defined in the body of the Regulation, since it is often what gives rise to risk. It might be appropriate to mention profiling, which seems to be the intended reference of these provisions.

At (c) of the same paragraph: the scope of this provision on video surveillance should be clarified. Lastly, the processing of sensitive data should also appear in the list of operations presenting specific risks. We would therefore like a subparagraph added to paragraph 2.

We have a scrutiny reservation on paragraph 3.

On paragraph 5, we would like the exception not to be restricted to Article 6(1)(c) but also to cover the case of Article 6(1)(e) on operations carried out in the public interest or in the exercise of official authority, and also the processing for historical purposes referred to in Article 6(2).

Article 34 - Prior authorisation and prior consultation

In general, we refer back to our remarks on Article 33 and the fact that we are uncertain of the relationship between that Article and Article 34. Taking these Articles together, as they stand, the distribution of tasks between controller, processor and data protection authority cannot be understood.

In general, we consider that this Article should be expanded to provide for other forms of consultation of the supervisory authority (declaration, opinion) than the current procedure.

Still as a general comment on this Article, we note that it gives excessive powers to the supervisory authority (authorisation, prohibition, publication of the list of processing operations that must be submitted to it). It also seems contrary to the aim of making the Regulation uniform if each supervisory authority draws up the list as it sees fit. Lastly, in any case, this Article should clarify the obligations of the controller when the list is modified: what happens to processing operations in progress? Must the supervisory authority be consulted?

At the same time, this Article reduces too far the formalities that any controller has to go through with the supervisory authority before implementing a processing operation. We understand that this Article abolishes the declaration and opinion procedures and that only the authorisation procedure remains, since it applies only to processing operations for which an impact assessment is required and those that may present specific risks with regard to the rights and freedoms of the data subjects for whom a list is established. We think that the simplification of administrative tasks should not mean being dispensed from the obligation to notify the supervisory authority and that on the contrary a mechanism should be provided to allow the supervisory authority to be aware of all controllers, inter alia for the sake of effective downstream supervision once the processing operations are implemented, but also for the sake of greater legal certainty for controllers. A simplified declaratory notification system could also be considered, along the lines of that allowed for by Directive 95/46 (which would not imply a power of prohibition for the supervisory authority) for other processing operations, with Member States having the power to decide the scope of that system.

We also stress that the ending of the prior opinion procedure could lead to problems with certain **administrative files**, which would no longer be subject to the declaration procedure but only the authorisation procedure. The distinction between files subject to authorisation and those subject only to an opinion should be maintained. It would thus be necessary to have an opinion procedure for some processing operations, which would exclude the possibility of prohibiting those operations.

Lastly, we wonder about the time limit for the supervisory authority to give its decision when it is consulted or receives a request for prior authorisation. In French law, the period allowed is two months.

Regarding the old paragraph 1, now moved to Article 42(6), we would point out that the wording be changed, replacing "*to mitigate the risks*" with "***to ensure that the necessary steps to minimise*** *the risks*" have been taken. However, we welcome the deletion of this paragraph from Article 34.

We would also like to know why this paragraph applies only to data transfers to third countries.

In conclusion, we would like this paragraph reworded to be clearer.

We would also like to know the scope of the consultation of the supervisory authority. Does the authority issue opinions (perhaps published) when consulted, or does this Article merely require cooperation between the controller and the supervisory authority, so that the processing complies with the provisions governing personal data protection?

Lastly, on (b), we think it would be desirable for the list of processing operations for which the supervisory authority has to be consulted to be established by the EDPS. This would make possible greater consistency in the application of the Regulation in the various States (see comments on paragraph 4).

In the same paragraph, as stated above, "*garantir*" should be replaced by "*assurer*" in the French text.

As regards the addition of "*except where a data protection officer has been designated in accordance with Article 35*" at the end of paragraph 2, we are entirely against this exception. The designation of a data protection officer should not exempt a controller from the requirement to conduct an impact assessment in the situations envisaged.

On paragraph 3, we believe that in some cases the supervisor need not make appropriate recommendations. We therefore propose that "if necessary" be added in this paragraph:

"*Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and**, if necessary,** make appropriate proposals to remedy such incompliance*."

We also think that the consequences of this opinion of the supervisory authority should not be the same for private data processing controllers and public authorities, in line with French law. We therefore propose specifying the consequences of this opinion:

- for enterprises, a negative opinion would be binding and should prevent the enterprise from implementing the data processing operation, as was envisaged in the original version;
- for public authorities, though, the opinion would not be binding but should be published.

On paragraph 4, we also stress that we have reservations on its being solely for the supervisory authorities to define the processing operations which are subject to prior consultation, and on the risk of divergences between the lists produced by different supervisory authorities in the cases other than those stipulated in paragraph 5, for which the supervisory authorities must implement the consistency mechanism provided for in Article 57.

We would like clarifications as to the consequences of communicating the list to the European Data Protection Supervisor. Is the idea to avert the risks of divergences between supervisory authorities? How, and what would the role and powers of the EDPS then be?

On the old paragraph 7, moved to paragraph 52(1)(f), we still have questions about the scope of this provision regarding the consultation of the supervisory authority on regulatory or legislative measures.

In paragraph 8, the notion of "*high degree of specific risk*" should be defined in the context of this Regulation, not in that of a delegated act.

Section 4 – Data protection officer

By way of a general remark on all the articles in this section of Chapter IV of the proposed Regulation, we **stress that we refuse to have the designation of a data protection officer become a requirement, and we insist that it remain an option, particularly for public authorities.** We consider that it is not for the European Commission to interfere in the internal organisation of the Member States by imposing the requirement of a data protection officer within that administration.

Article 35 - Designation of the data protection officer

In paragraph 1, we would like clarification on the first sentence, as to whether the objective is a designation for both the controller and the processor or the designation of one officer for each.

On point (a) of that paragraph. we note that the requirement to designate a data protection officer is imposed on all public authorities or bodies, but not on enterprises employing fewer than 250 persons, inter alia because of the cost of such a measure. We would therefore like clarifications of what justifies the fact that there is no similar exemption from the requirement to appoint a data protection officer for smaller public authorities or bodies. We find this designation requirement too burdensome and unsuited to small organisations, such as some departmental archive departments in public bodies or even in small departments with nationwide responsibilities.

In paragraph (1) point (c), the criterion that "*the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects*" is unclear, insufficiently discriminating and would allow almost all enterprises to be included. To prevent every article having to include specific criteria, it would thus be useful to include a criterion relating to risk, so as to make this Article consistent with the rest of the Regulation. This presupposes that risk has been defined.

In paragraph 3, to be able to assess the proposed flexibility, we would like clarification on what is meant by "*taking account of the organisational structure of the public authority or body*".

In paragraph 5, we consider that there is a potential contradiction between expert knowledge of data protection law and practices, and the level of expert knowledge determined by the data processing carried out.

In paragraph 6, we wonder about the concept of "*conflicts of interest*" in this paragraph and would like clarification in order to understand its exact meaning. We wonder in particular about the additions to this paragraph, and about other tasks and duties which could be assigned to a data protection officer who is not an employee or civil servant of the controller.

In paragraph 7, we consider that the Cyprus Presidency's proposed addition ("*apart from serious grounds under the law of the Member State concerned*") does not make it clear enough that Member States' national employment law, which this Regulation is not intended to govern, must be taken into account. The addition would make it possible to dismiss a data protection officer under other circumstances than those envisaged in the Regulation, on the basis of serious grounds provided for in national law. We would like further information on what is meant by the expression "*serious grounds under the law of the Member State concerned*". We would also like clarification on which national law would apply if the designated data protection officer is not located in the same Member State as the controller given that, under the amended Article 35(6), the officer might not be an employee of the controller. In addition, we consider the proposed addition to this paragraph is too limited and we prefer a more general reference to the fact that Member States' national employment law must be taken into account.

Article 36 - Position of the data protection officer

We would refer here to our general comments, set out above on this section as a whole and, with regard to this article in particular, we would add that employment as an official or civil servant does not seem compatible with the requirement in paragraph 2 for the data protection officer to be independent.

In paragraph 2, we wonder about the concepts of "*management of the controller or the processor*" and its proposed replacement "*head*", and question the coherence between this paragraph and the next, in particular the prohibition laid down in paragraph 2 alongside the obligation in paragraph 3 for the controller or processor to support the data protection officer in performing tasks, as well as the requirement to entrust the data protection officer with tasks as provided for in Article 37. Moreover, if the concept of independence referred to in paragraph 2 is the same concept covered by Directive 95/46, we consider that it would be appropriate to clarify the proposed provision in order to ensure that it is properly implemented.

With regard to paragraph 3, we consider it should be clarified that the support provided by the controller or the processor is in the form of material supplies and equipment. Thus the words "*and shall provide*" should be amended and replaced by the words "*by providing*".

Article 37 - Tasks of the data protection officer

In paragraph 1, we would like to add a point to the list of the data protection officer's tasks, specifying the obligation to draft an annual report for the controller, as indicated in footnote 468.

Section 5 - Codes of conduct and certification

By way of a general comment on the two articles in this section of Chapter IV, we are in favour of the facilitation tools for companies laid down in the proposed Regulation, which should enable businesses to fulfil their obligations in a flexible and appropriate manner while integrating developments, particularly in terms of technology. However, we question the scope of these tools and, in particular, their mandatory nature and, where applicable, the appointment of those responsible for ensuring the uniformity of local provisions. Furthermore, Articles 38 and 39 concern businesses more specifically, which makes us wonder about how these provisions apply to the authorities and public bodies.
Finally, as we have already mentioned on several occasions, we do not agree that the Commission should be empowered to adopt delegated acts or implementing acts whose content could be included in the text of the Regulation itself.

Article 38 - Codes of conduct

We propose that codes of conduct must be approved by the supervisory authorities before they are published.

In paragraphs 2 and 3, we wonder what is meant by "*associations and other bodies representing categories of controllers*".

In addition, we support the German delegation's proposal (footnote 469 of the Presidency compromise) to provide a derogation for the public sector. Paragraphs 2 et seq. do not seem suitable for the public sector.

In paragraph 4, we are unsure as to the legal value of codes of conduct, since paragraph 1 does not seem to confer any binding force on them and yet the Commission may decide on the basis of paragraph 4 that the codes of conduct have general validity within the Union.

Article 39 - Certification

We have reservations about certification at national level and would prefer European certification.

We wonder about the range of terms used in this article: "certification", "marks" and "seals". These terms cover different concepts and we consider that the wording of this article should be made clearer. They do not involve the same processes or the same requirements, nor is compliance monitored by the same bodies.

We also consider that the article is insufficiently precise with regard to monitoring compliance with certification. The article focuses on the establishment of certification mechanisms but does not make any provisions for monitoring "certified" controllers' compliance with the criteria, even though regular monitoring is necessary. If there are no checks, controllers who obtain certification could be tempted to display their certification without continuing to comply with the criteria which enabled them to obtain it.
We would therefore like the supervisory authority to be empowered to monitor compliance with the certification process. In connection with the above comment on the range of terms used in this article and on the range of specific bodies responsible for monitoring compliance with the procedure for seals, certifications and marks, this point should also be clarified.

ITALY

Article 30

In the title of the article, we propose deleting the reference to "*confidentiality*": the provisions in question are intended to define security measures applicable to the processing of personal data, as opposed to the confidentiality criteria for data relating to staff employed by the controller/processor or other parties, which need to be processed.

In paragraph 1, the phrase "*including the use of pseudonymous data*" should be deleted (describing this category as a security measure is inappropriate; this issue is also ongoing, as regards the inclusion of an express reference to data of this kind in the wording of the Regulation). The words "*confidentiality and*" should also be deleted (for the reasons given above regarding the title of the article).

We would propose deleting paragraph 2a (see above).

We agree with the proposed deletion of paragraphs 3 and 4: as mentioned previously, the fact that the Commission is empowered to adopt delegated acts as regards security measures causes confusion.

Article 31 - Notification of a personal data breach to the supervisory authority

Paragraph 1: we agree with the amendment concerning the "*fundamental rights and freedoms*" of data subjects, designed to limit the supervisory authority's involvement to cases involving actual risks.

As regards the 72-hour time period referred to in the proposal for a regulation, it would be worth aligning this period with the provisions made in Directive 2002/58/EC (the E-Privacy Directive), which also covers data breaches, in order to achieve a single system for notifying authorities, for both the electronic communications and data protection sectors.

Paragraph 3: we would propose adding the following phrase to point (e): "*describe… to address the personal data breach, including the measures referred to in Article 32(3)*"; this would provide the authority with a complete framework for the processing operation in respect of which a breach has occurred (in accordance with Article 31(4)).

For paragraph 4, we would propose adding an explicit reference to the need to assess the severity of the breach using the information which the controller is required to document: "*The controller shall document… comprising the facts surrounding the breach, its effects, the estimated severity and the remedial action taken*".

Article 32

Paragraph 1: we agree with the amendment proposed by the Irish Presidency (5702/13).

Paragraph 3: we would propose deleting the addition "*such as encryption or the use of pseudonymous data*", as it is excessively prescriptive and would be better placed in recital 68a, in keeping with the proposal made by the Irish Presidency (5702/13).

Article 33

The proposal for a regulation states that the controller is obliged to assess the impact on the protection of personal data in cases of processing operations which present specific risks. In order to avoid making this impact assessment a purely formal and administrative procedure, we would describe as appropriate the statement added in paragraph 1 by the Irish Presidency (5702/13), in accordance with which the performance of these impact assessments is made subject to account being taken of a whole range of risk factors such as the nature, scope and purposes of the processing and possible adverse effects (in accordance with recital 70).

We agree with paragraph 1a (added by the Irish Presidency, 5702/13) on the grounds that the aim is also to restrict such assessments to cases where the controller/processer has not appointed a data protection officer (DPO) in accordance with Article 35(4). However, this amendment requires the DPO, as indicated in Article 37, being expressly authorised to perform the impact assessment (if appropriate) (see below).

With regard to paragraph 2 and the list of processing operations which present specific risks, we have the following comments to make for each point: in point (a) we would propose deleting the words "*on a large scale*"; for point (b) we would propose including a reference to Article 9(1) (in fact, the processing of any of the categories of sensitive data would require an impact assessment specifically relating to the particular nature of the data concerned). The reference to "*on a large scale*" should also be deleted from points (b), (c) and (d). In point (c) we would suggest removing the reference to "*video surveillance*".

The introduction of paragraphs 2a and 2b by the Irish Presidency (5702/13), taken from Article 34(4) and (5), is acceptable, provided that it is not considered to have been replaced by those paragraphs, for the reasons given in our comments on Article 34 below.

Article 34

Paragraph 2: the proposal made by the Irish Presidency (5702/13) limits the requirement for prior consultation of the supervisory authority, to the cases indicated in Article 34(2)(a) of the original proposal, i.e. where the result of the impact assessment has been "negative".

However, the new wording is excessively restrictive as regards the requirement for prior consultation of the Authority for other types of processing operations, to the detriment of the protection of the rights of data subjects. This results in the limitation or even prevention of the possibility of a European list of processing operations involving specific risks (different from those linked to the factors described in Article 33(2)), a possibility which would be a major step forward in terms of legal certainty and harmonisation.

Therefore, as mentioned above in our comments on Article 33, we feel it necessary to maintain paragraphs 4 and 5 of Article 34 of the original text.

With regard to paragraph 3, the reference to specific periods for consultation (six weeks) would appear to be more a detail rather than a general point and in any case would appear to be excessively prescriptive.

We have doubts surrounding the fact that the supervisory authority is no longer able to prohibit a processing operation if it does not comply with the Regulation. It is also unclear what the consequences of the "*appropriate recommendations*" made by the supervisory authority would be. The obligation regarding prior consultation is not binding. It would therefore seem advisable for this paragraph to include a reference to Article 79(5)(m), or, more generally, to the supervisory authority's powers under Article 53(1).

We agree with the other proposed amendments made in document 5702/13.

Article 35(1)(b), (7),(8) and (9)

We agree with the amendment proposed by the Irish Presidency in 5702/13, provided that the criterion set out in paragraph (b) is not separated from that indicated in paragraph (c).

In any case, it would be worth taking account not just of the number of persons employed by an enterprise, but also the nature and scope of the processing of personal data, and also the number of staff directly involved in the processing operation and/or the number of data subjects.

The Irish Presidency's proposal only takes account of some of the demands made regarding a more flexible wording and therefore further reflection on this matter would be worthwhile.

In particular, there is significant confusion surrounding the fact that paragraph 8 has remained unchanged and the introduction in paragraph 9 of the words "*upon request*", since the existence and appointment of an DPO within an organisational structure should be the subject of maximum transparency and accessibility.

Article 36

We agree with the amendments proposed by the Irish Presidency (5702/13): the amendment in question ensures a sufficient and equilibrated balance between the duties/powers of the controller and those of the DPO, ensuring that the requirements of simplification, operational flexibility and enterprise autonomy are complied with.

Article 37

Paragraph 1: for the reasons already outlined in our comments on Articles 33 and 34, we would propose that the list of the DPO's responsibilities also include a reference to performing data protection impact assessments for the cases mentioned in Article 33(2)(a).

Article 38(4)

We would point out the useful potential role of the European Data Protection Board as regards codes of conduct. We would therefore propose requiring the Commission to consult the Board and obtain its approval on the subject of codes of conduct at European level (as also suggested by the European Parliament).

Article 39(1)

The involvement of the European Data Protection Committee would be welcomed, including with regard to monitoring the development of certification systems by means of data protection-friendly seals and signatures.

LATVIA

The Ministry of Justice of the Republic of Latvia expresses gratitude for the proposed drafting of 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). Latvia supports proposals presented by the Commission to modernize EU data protection regulation, especially, considering the fact that the current legislation has been adopted more than 16 years ago. Furthermore, it is necessary to pay attention to rapid developments in the field of information technologies and its role in nowadays society. The new regulation will strengthen data protection in the EU and create modern, strict and consequent regulation for data protection.

In response to invitation of the Presidency to submit comments on Article 28 to Article 39 of the General Data Protection Regulation:

1. Latvia has previously expressed concerns that competences of the Commission, in respect to the issuance of delegated legal acts, stated in the current regulation can cause legal uncertainty due to their often and wide usage that prolong implementation of the regulation. Thus it would be advisable to evaluate the division of competences between Member States and the Commission. The competence to solve technical issues has to be left to the Commission, but substantial issues have to be discussed within the context of the instrument.

As for Articles 28 to 39 Latvia would like to propose to delete the words '*to take account of in particular the responsibilities of the controller [and the processor] and, if any, the controller's representative*' from the Paragraph 5 of Article 28. The documentation described in the Subparagraph 2 of Article 28 also points to the responsibilities of the controller, processor and controller's representative that has to be observed to gather the documentation; therefore there is no further need to adopt delegated acts concerning this matter.

2. Latvia has previously emphasized necessity to avoid cases when the assignment of data controller is formal by its character, meaning, when the amount of data processed in one entity is very small or in opposite – when the amount of data processed in one entity is remarkable and it is inadequate to assign only one data controller.

Therefore Latvia would like to propose to delete Subparagraph 1 (b) of the Article 35. Latvia considers that the criterion for designating the data protection officer can't be 'employing 250 persons or more'. The criteria for designation of the data protection should be based on risk approach – the amount and type of data processed.

LITHUANIA

General Remarks

Lithuania supports Presidency direction on General Data Protection Regulation to work on risk based model. Our position in most cases is in line with proposed amendments in Presidency draft document No. 5702/13 published on 28 January 2013 (articles 28, 30, 32, 33 par. 4, 34 par. 4, 5 etc.). As regards the delegated and implementing acts in the relevant articles our position which was expressed before has not changed. However, there are some comments we would like to share with.

Comments and proposals on the Regulation article by article

Article 29

We welcome the proposed deletion of Article 29 as we share the view that this article is superfluous taking into account other provisions in the Regulation.

Article 30

Article 30 paragraph 3 states that the Commission is empowered to adopt delegated acts in accordance with Article 86 of the proposal. Lithuania, however, believes that the requirements for technical and organisational measures should be determined by national law not by delegated acts.

Article 31

Article 31 paragraph 6 states that the Commission may lay down the standard format of notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Taking into account all the aspects of independence of national data protection authority laid down in the Regulation, we think that the requirements and obligations regarding notification should be set within Regulation.

Article 35

We reiterate that the appointment of data protection officer in public institutions or private organizations, if they employ more than 250 people, have to remain voluntary as it is currently in Directive 95/46/EC, and not to become a duty. Having expressed that, we welcome improvements in Articles 35 to 37 presented by the Presidency. We strongly share the ideas that there should be a possibility for several public entities to appoint one data protection officer (amendment of Article 35 paragraph 3) and that there should be left manoeuvre for private or public entities to appoint such officer from the personnel already involved in the similar activity of company (lawyers etc.) (amendment of Article 35 paragraph 8).

Article 36

We would like to suggest the following amendment of paragraph 3, because we see it as being too prescriptive:

"The controller or the processor shall support the data protection officer in performing the tasks and shall provide ~~staff, premises, equipment and any other~~ resources necessary to carry out the duties and tasks referred to in Article 37.

LUXEMBOURG

These comments are without prejudice to any further comments made in subsequent negotiations.

The general remarks made in earlier written comments remain valid.

Luxembourg would like to underline its support of a risk-based approach and considers the Presidency proposal in document 5702/13 an excellent basis.

Detailed comments/questions

Article 28 – Documentation

Luxembourg believes that this article nullifies the abolition of the notification obligation and needs to be more nuanced in order to avoid disproportionate administrative burden. Luxembourg also continues to regard the exemption for controllers with more than 250 employees as arbitrary. Rather, the obligation to document should also be articulated with the risk-based approach. Particularly for more risky processing, controllers should be able to demonstrate compliance with this article.

The respective allocation of obligations and responsibilities between controllers and processors needs to be clarified. It should be avoided that a same processing is documented twice by a controller and a processor.

Article 28

Documentation

1. Each controller ~~and processor~~ and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

Article 29 – Cooperation wit the supervisory authority

Luxembourg considers this article as self-evident and is not convinced by its added value.

Article 30 – Security of processing

The respective allocation of obligations and responsibilities between controllers and processors needs to be clarified. According to Luxembourg, the controllers should have the prime responsibility. Therefore Luxembourg proposes to delete the reference of "the processor" in paragraph 1 and to insert a new paragraph 2 which is in fact the reintroduction of paragraph 2 of Article 17 of the directive 95/46. While avoiding an unnecessary multiplication of different security measures and standards used in a given processing, this does not preclude that depending on their role in the processing, different measures could be adopted by the controller and the processor (as clarified in their contractual relationship).

Article 30

Security and confidentiality of processing

1. The controller ~~and the processor~~ shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

   (…)

2. (new) The controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures

In paragraph 2, Luxembourg wonders whether the "evaluation of risks" is the same one as the data protection impact assessment of Article 33.

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

Luxembourg considers it necessary to set a threshold: only personal data breaches seriously affecting the data subject should be deemed necessary to be notified, in order to avoid "notification-fatigue" and to keep the provision efficient and result-oriented. Luxembourg is also skeptical about the 24-hour deadline: in case of a personal data breach, the first priority of controllers and processors should be to remedy the breach and not to file a substantive notification to the DPA. It is also unrealistic to expect that within 24 hours the full consequences and necessary mitigating measures are fully known. The content of the notification should be adapted and take a more proportional and pragmatic approach.

Article 33 – Data protection impact assessment

Luxembourg wonders what is meant by "*specific* risks" in paragraph 1. As this article may be the anchor of the risk-based approach, it would be useful to define such risks for the data subject (eg. identify theft, financial loss etc).

The respective allocation of obligations and responsibilities between controllers and processors needs to be clarified. It should be avoided that an impact assessment has to be carried out twice – by the controller and the processor - for a same processing.

Luxembourg also wonders at what moment such an impact assessment should be made: once before a given processing, when the purposes of a processing change or when new means of processing are used?

Article 34 – Prior authorisation and prior consultation

The respective allocation of obligations and responsibilities between controllers and processors needs to be clarified. It should be avoided that prior authorization and prior consultation would be requested twice, potentially in different jurisdictions.

In paragraph 4 and 5, Luxembourg is concerned that the drawing up of such lists by each DPA will lead to incoherencies and should therefore be done at EU level.

Article 36 – Position of the data protection officer

Luxembourg wonders about the notion “independent” and in relation to whom/what the DPO is supposed to be independent. It should also be permitted that the DPO can occupy other functions, as long as there is no conflict of interests. Further, it is important to allow for DPOs to be outsourced by controllers, particularly for SMEs. Finally, Luxembourg also supports proposals that DPOs may be shared by a group of undertakings or several administrations.

Article 38 – Codes of conduct

While Luxembourg fully supports that the drawing up of industry-led codes of conduct should be encouraged (also in support of a technologically neutral and future proof Regulation), and be part of a risk-based approach, the normative value of this article is unclear.

NETHERLANDS

(64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to lead to present a high degree of risk, the controller or the processor shall be responsible to perform a data protection impact assessment. The outcome of the assessment shall determine the extent of the requirements on documentation, security standards, the notification of data breaches and the need to designate a data protection officer.

(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to cooperate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations. If the outcome of a data protection impact assessment indicates the processing operation presents a high degree of risk a more detailed documentation requirement is justified.

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred in processing operations which present a high degree of risk according to the outcome of a data protection impact assessment, the controller should notify the breach to the supervisory authority without undue delay (…). 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.

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, the controller must ascertain whether all appropriate technological protection and organisational measures have been applied and implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(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 mechanism 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. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which 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.

(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.

(74) (…)

(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which present, according to the outcome of a data protection impact assessment a high degree of a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks autonomously.

(76) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors.

(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

Article 28

Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. Where a data protection impact assessment as provided for in Article 33 indicates the processing operation presents a high degree of risk, referred to in Article 33, the documentation shall contain at least the following information:

   (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

   (b) (…);

   (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

   (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

   (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

   (g) where relevant, a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) a natural person processing personal data without a professional gainful interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. (…)

6. (…)

[1]

SECTION 2
DATA SECURITY

Article 30

Security of processing

1. The controller (…) shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

[1] NL believes that Chapter VI sufficiently regulates the relations between data controller, processor, representative and DPA.

2. The controller (…) shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

(2a) Where personal data are processed on behalf of the controller by a processor, the contract or other binding legal instrument which governs relations between the controller and the processor, referred to in Article 26, paragraph 2, must contain binding provisions which require the processor to abide with the duties referred to in paragraphs 1 and 2.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 31

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach in processing operations where a data protection impact assessment as provided for in Article 33 indicates that the processing operation presents a high degree of risk as referred to in Article 33, the controller shall without undue delay after having become aware of it, notify the personal data breach to the supervisory authority.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. The notification referred to in paragraph 1 must at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data controller (…) where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. (…)

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach, referred to in Article 32 is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates (…) that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. (…)

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

1. Where processing operations <u>are likely</u> to present <u>a high degree of risk</u> to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes<u>, or the scale of the operations</u> the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations (…) present a high degree of risk referred to in paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(c) personal data in large scale filing systems on children, genetic data or biometric data.

2a. A high degree of risk referred to in paragraph 1 and 2 is present, when the processing operations are likely to imply a substantive risk of:

(a) identity theft;

(b) substantive financial loss of the data subject or third party;

(c) loss of confidentiality of bank or creditcard account numbers of the data subject or third party;

(d) discrimination of the data subject or third party;

(e) loss of confidentiality of data protected by a professional secrecy regulated by Union or Member State law;

(f) serious moral damage to the data subject or third party.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the 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 the Articles 28, 30, 31, 32, and 35 of this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union or Member State law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. The Commisson shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying processing operations that by their nature represent a high degree of risk, referred to in paragraph 1.

Article 34

Prior authorisation and prior consultation

[1]. (…)

[2]. (…)

[3]

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body; or

   (b) a data protection impact assessment as provided for in Article 33 indicates processing operations present a high degree of risk, referred to in Article 33.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

---

[1] NL suggests the transfer of Article 34, paragraph 1, to Article 42.

[2] NL suggests deleting Article 34, paragraphs 2, 3, 4 and 5, since prior consultation leads to overburdening DPA's en does not offer any additional legal certainty, while prior authorisation is only a useful tool in Chapter V of the Regulation. Paragraph 6 of Article 34 can be transferred to Article 33.

[3] NL suggests to regulate the position of the DPA in the domestic legislative process in Article 52.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks autonomously and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

Article 37

Tasks of the data protection officer

The controller or the processor shall entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, data protection awareness raising, the training of staff involved in the processing operations, and the related audits;

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security; (…)

(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to perform a data protection impact assessment if the controller or processor request him to do so and the application for prior authorisation , if required pursuant Articles 33 and 42;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, cooperating with the supervisory authority at the latter's request or on the data protection officer’s own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

Article 37a

Powers of the data protection officer

1. The controller will entrust the data protection officer with to power to inspect any data processing operation carried out under his responsibility and the right of access to all data processed.

2. The data protection officer may not further process any data to which he has gained access in the exercise of his duty, except on instructions of the controller, unless he is required to do so by Union or Member State law.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;

(b) the collection of data;

(c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights;

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 39

Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

POLAND

Comments on Annex I to 5702/12

Article 28

Documentation

1. Each controller **(…)**and, if any, the controller's representative, shall maintain documentation***, in the form of paper or electronic document,*** of all **categories of** processing activities under its responsibility.

2. **This** documentation shall contain (…) the following information:

   (a) the name and contact details of the controller, any joint controller or processor, and of the **controller's** representative, if any;

   (b) the name and contact details of the data protection officer, if any;

   [(c) the purposes of the processing [including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)];

   (d) a description of categories of data subjects and of the categories of personal data relating to them;

   (e) the **(…)** categories of recipients of the personal data **(…)**;

   (f) where applicable, **the categories of** transfers of **personal** data to a third country or an international organisation, **(…)** and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

   (g) a general indication of the time limits for erasure of the different categories of data;

   (h) **(…)**

2a. Each processor shall maintain the documentation of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the categories of processing carried out on behalf of each controller;

(d) where applicable, the categories of transfers of personal data to a third country or an international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards.

3. **Upon request, t**he controller [and the processor] and, if any, the controller's representative, shall make the documentation available (…) to the supervisory authority.

4. The obligations referred to in paragraphs 1**, (…)** 2 **and 2a** shall not apply to:

(a) (…)

(b) (…)

(c) categories of processing **activities** which are unlikely **to represent risks for** , the fundamental rights and freedoms of data subjects **by virtue of the nature, scope or purposes of the processing**;

5. **(…)**

6. **(…)**

Comments PL:

Due to the fact, that the references to the delegated act which may specify the form of documentation were deleted, in PL view it is necessary to define in the Regulation the possibility of electronic form of documentation. Lack of legal clarity in this matter may jeopardize the contractual certainty and bring unnecessary burdens for controllers or processors. PL welcomes new provisions dividing the requirements for the controllers and processors, as well as new criterium for exemptions of maintaining documentation by these bodies.

Article 29

Cooperation with the supervisory authority

(…)

Comments PL:

PL supports the deletion of this article.

SECTION 2

DATA SECURITY AND CONFIDENTIALITY

Article 30

Security and confidentiality of processing

2. (…)

2a. **The obligation of confidentiality on any person acting under the authority of the controller or the processor shall continue to have effect after the termination of their activity for the controller or processor**

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

Comments PL:

PL supports keeping the references to the delegated acts in this article provided that the new recitals limit the issuing of delegated acts by the Commission, In the context of rapidly developing technologies and standards it is rather important to ensure the appropriate level of technical solutions, the use of which provides real data security, rather than recent existing solutions. Standards used in the Member States may differ, so determining "the latest standards" of the EU would certainly adversely affect the functioning of companies in Poland. Besides PL welcomes encryption and pseudonomisation as a way to ensure the data protection by the controller and processor.

Article 31

Notification of a personal data breach to the supervisory authority

Comments PL:

PL supports the changes in the text, which are aimed at inserting the evaluation criteria for the personal data breach. PL also welcomes new period for the notification of data breach which is more realistic.

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the **fundamental rights and freedoms** of the data subject, the controller shall (…)communicate***, in the form of paper or electronic document,*** the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (f)of Article 31(3).

3. Notwithstanding paragraph (1), the communication of a personal data breach to the data subject shall not be required if the controller (…) has implemented appropriate technological protection measures and **(…)** those measures were applied to the data **affected by** the personal data breach. Such technological protection measures shall **include those that** render the data unintelligible to any person who is not authorised to access it**, such as encryption or the use of pseudonymous data**.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

[5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

Comments PL:

PL supports the changes already made, but would also point out to keep under consideration the possibility of introducing the electronic form of communication in the Regulation itself, similarly to art. 28.
PL supports keeping the references to the delegated acts in this article provided that the new recitals limit the issuing of delegated acts by the Commission in this area.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

Comments PL:

With the view of limiting the unnecessary burdens for processor PL is opposed of expanding data protection impact assessment on the processors. PL also welcomes deletion of paragraph 4.

Article 34

Prior authorisation and prior consultation

Comments PL:

PL supports the amendments which were introduced in paragraphs 3 and 6. But would like to put scrutiny reservation to new paragraph 3a. These provisions create considerable legal uncertainty for business. PL also supports keeping the references to the delegated acts in this article provided that the new recitals limit the issuing of delegated acts by the Commission in this area.

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

Comments PL:

PL supports the amendments which were introduced in this article towards more flexibility in designating data protection officer. The criterion of size of the enterprise should not be the sole criterion.

Article 36

Position of the data protection officer

Comments PL:

PL supports the amendments.

Article 37

Tasks of the data protection officer

Comments PL:

PL supports the amendments.

SECTION 5

CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

Comments PL:

PL supports the amendments.

Article 39

Certification

Comments PL:

PL supports the view of BE, SI and NL that certification should take place mainly on a voluntary basis.

PORTUGAL

Article 28 Documentation

Article 28(4)(b) contains a drafting error (which only affects the Portuguese version of the document): the document reads "*mais de 250 assalariados*" ("employing more than 250 persons"), whereas it should obviously read "*menos de 250 assalariados*" ("employing fewer than 250 persons").

The exception provided in Article 28(4)(b) should be reviewed. In fact, the obligation in question relates to the requirement to document the processing of personal data: it is not clear why a company would be exempt from this documentation obligation on the grounds of employing fewer than 250 people. This is a number like any other which the Commission has decided to use, whereas it could have opted for another one, a conclusion reached during the discussions by DAPIX (Working Party on Information Exchange and Data Protection). Other criteria could and should be used, such as the volume and the type of data processed. The need not to create excessive burdens for both the public and private sectors should also be taken into account.

Article 30 - Security of processing

This article presents points of confluence with Chapter III-A "Security and Integrity of networks and services", from the consolidated version of Directive 2002/21/CE, transposed into national law by Chapter V of Law n. 5/2004, February 10, in drafting amended by Law n. º 51/2001 of 13 September, as well with the regime of Directive 2002/58/CE, amended by Directive 2009 / 136/CE. In this context it is important to clarify whether the regime of the Regulation does not expand or alter the arrangements of the mentioned legal instruments.

Article 31 Notification of a personal data breach to the supervisory authority

The Directive 2002/58/EC on the consolidated version provides that in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority (article 4 (3)). As for the elements to be included in the notification to the supervisory authority, they not always coincide with what is stated in the Regulation.

The notification deadline proposed in the Regulation embodies something that was not defined in the Directive. Regarding the elements of notification (although the data in question may be the same, in the sense that these are personal data), the terms of the notification may be distinct.

It would be important to clarify the relationship between the provisions, namely as a way to reduce costs for operators and prevent unnecessary duplication, contrary to the spirit of the rest of this Regulation.

It should be noted that ENISA (European Agency for Network and Information) has also drafted in December of 2011 a recommendation on the implementation of article 4 of Directive 2002/58/CE.

Finally, regarding the communication of data breach to its holder (article 32 of the Regulation), the procedure is similar to the Directive.

The "criteria and requirements" referred to in paragraph 5 should be established after an opinion issued by the European Data Protection Board. We would prefer this type of decision to fall within the Council's remit, though on the basis of a Commission legislative initiative.
We agree with the rest of the Commission's proposed wording for the Article, including the use of delegated acts for the purposes stated in paragraph 6.

We agree with the rest of the Commission's proposed wording for the Article, including the use of delegated acts for the purposes stated in paragraph 6.

Article 32 Communication of a personal data breach to the data subject
The comments made above concerning Article 31 also apply to paragraphs 5 and 6 of this Article and the rest of the Article.

Article 33 Data protection impact assessment
The Directive 95/46/EC established a general obligation of notification of personal data to the supervisory authorities. The Commission considers that this obligation, in addition to give administrative and financial burdens, not always contributed to an improvement in the protection of personal data.

Therefore, this general obligation is deleted on the Regulation and replaced by procedures and mechanisms considered more effective related with the processing operations that present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purpose.

In such cases, the controller or the processor acting on the controller's behalf shall, prior to treatment, carry out an assessment of the impact on the data protection and consider, inter alia, measures, safeguards and mechanisms for ensuring the protection of personal data and verify the compliance with the Regulation.

It is noteworthy the possible need to clarify its articulation with the Directive 2002/58/CE.

Assessing the impact on data protection includes information on health. However, the criteria and conditions for data processing operations likely to present specific risks relating to the evaluation of aspects related to personal health or treatment information intended to provide health care and epidemiological investigations are specified by the Commission, through the adoption of delegated acts. Thus, it is suggested to clarify these criteria and conditions in the text of the Regulation and the elimination of the reference to delegated acts.

We agree with this Article, with the exception of paragraphs 5 and 6. We would reiterate the comments made above in connection with paragraphs 5 and 6 of Article 31.

However, we take the view that it is important that small and medium-sized enterprises, and particularly micro-enterprises, be taken into account, if they will potentially be required to conduct impact assessments.

Article 34 Prior authorisation and prior consultation

Article 34 should also provide the terms and conditions under which consultations are held with the national supervisory authority, since it does not mention deadlines and delegates in the Commission further specifications.

The production process of European and national Official Statistics by national and European authorities should be exempt from the obligation of prior consultation considering the specificity of theirs activity.

We agree with this Article, with the exception of paragraphs 5 and 6. We would reiterate the comments made above in connection with paragraphs 5 and 6 of Article 31.

Article 35 Designation of the data protection officer

We welcome the establishment of this position.

We would disagree with the number of staff employed (250) that has been used as a criterion in Article 35(1)(b). The majority of European businesses employ less than 250 people and the criterion used would mean that almost all European businesses would not be subject to this Regulation. We propose reducing this figure to 50 persons.

The data protection officer should be appointed from among staff members employed by the undertaking or group (as indicated in paragraphs 2, 3 and 4).

If the data protection officer is an employee, he/she should have a legal status of independence in order to perform his/her duties without being subject to coercion or pressure of any kind.

The comments made in connection with Article 31(5) also apply to paragraph 11 of this Article.

Article 36 Position of the data protection officer

No remark. We agree with the text proposed by the European Commission.

Article 37 Tasks of the data protection officer

We agree with the text proposed by the European Commission.

The comments made in connection with Article 31(5) also apply to paragraph 2 of this Article.

Article 38 Codes of conduct

We fully agree with the text proposed by the European Commission, including the section relating to the possibility of issuing implementing acts, as indicated in paragraph 4.

Article 39 Certification

Certification, as well as codes of conduct, may have a very important role, and may on occasion result in subsequent impact assessments not being necessary.

The comments made regarding Article 31(5) and (6) also apply to paragraphs 2 and 3 of this Article.

ROMANIA

Art.28

Par (2)

The obligation to **keep documentation** is too complex for the controllers. RO expresses concerns that this obligation would lead to unnecessary administrative burdens. We would like that the documentation that controllers/processors/representatives are obliged to keep, be more concise and exhaustively provided, than the wording at par 2.

Par. 4(b)

RO considers as irrelevant the criterion **"staff number"** for determining the exception to the general documentation requirement. The risk of the processing should be the criterion to be taken into account and not that of the number of employees. RO proposes the deletion of this criterion and implementing a risk based approach criteria.

Par. (5) and (6)

We do not consider necessary that art. 28 be detailed by implementing and delegating acts, because the text of art. 28 already offers a clear picture regarding the requirements for the documentation. So many implementing and delegating acts would minimize the substance of the regulation's provisions.

Art. 29

RO agrees that art. 29 should be moved within the chapter governing authority control functions.

Art. 30

Par. (3) and (4)

RO considers that the criteria and requirements for technical and organizational measures shall be established only at principle level and each state shall make their own assessment of the costs involved.

RO would like that dimension of implementing costs should be in accordance with the identified risks.

Art. 31

RO believes that the deadline of **24 hours** for reporting a data breach to the supervisory authority is unrealistic and insufficient for a complete documentation of the circumstances of the incident and may even lead to bureaucracy. There is a risk that controllers will be more concentrated on observing the procedures and deadlines imposed by the regulation, instead of undertaking appropriate measures to diminish the consequences of the breach incident.

RO proposes that the deadline be extended.

Art. 32

RO supports the establishment of a simultaneous information, when a data breach took place, both for the supervisory authority and for the data subject.

Par (5)

Not necessary. The delegating act minimize the substance of the regulation's provisions.

Art. 33 and Art. 34

The provision is too burdensome, especially for micro and SMEs. RO proposes eliminating the obligation for micro and SMEs in what concerns performing a data protection impact assessment. However, RO is aware of the fact that some processing operations present risks, irrespective of the size of the controller, but appreciates that clear elements should be provided in order to identify the situations when such an assessment is strictly necessary and for SMEs it should be carried out in a way as not to impose costs.

Art. 35

Par. (1), b)

The criterion of **250 employees** is irrelevant when determining the necessity of appointing a DPO. This situation should be dealt with from the perspective of the risk that the processing implies, such as: purpose of the processing, volume and categories of personal data processed. Many big enterprises don't process in any way personal data as a main activity, so we do not see why a DPO is necessary in their cases.

Par. (11)

RO considers that the member states should establish the criteria and requirements for the core activities of the controller or the processor.

SLOVAK REPUBLIC

Article 22

In terms of legal certainty this Article has to be précised and completed directly in the text of the Regulation, or it is needed to publish the Regulation concurrently with an act in accordance to the Article 86.

Further, we consider as a necessary to amend Article 22 or another appropriate Article of the Regulation proposal, in the context of request and reservation of the Slovak Republic to introduction of a new concept *"entitled person"* in Article 4 of the Regulation proposal, the obligation for the controller and processor to instruct their entitled persons coming into the contact with personal data about rights and duties and liability for breaching them. Advice is needed to be done before giving the first instruction to the entitled person to perform any processing operation with the personal data. The controller or the processor shall make and store a written record of the advice.

The term "*accountability"* of the controller and the processor is rich in meaning. Therefore we suggest specifying more clearly the arrangements and mechanisms used to ensure the provisions of the Article 22(2). The Slovak Republic suggested defining a new term in the Article 4, in concrete „*entitled person*". Entitled person should be any natural person coming into the contact with personal data within the framework of his/her employment relationship, civil service employment relationship, membership, based on authorization, election or appointment or within the framework of performance of a public function, who may process personal data only upon instruction of the controller, controllers' representative or processor.

In the Paragraph 3 it seems as a necessary to define mandatory or minimal mechanisms for the verification of the provisions effectiveness adopted in the Article 22 (1) and (2) and also define the conditions on which the independent audit of these mechanisms will be required.

Other comments and suggestions to this article that were raised by the delegations at the meetings, we insist on.

Article 23

We suggest to replace the wording in Paragraph 1 of this Article "*at the time of the determination of the means for processing and at the time of the processing itself*" by the wording "*at least at the time before starting processing*". The controller is not the producer of new technologies, so it is necessary to formulate this paragraph so as he/she would be obliged to make appropriate technical and personal steps regarding the newest technologies and its economical availability before processing itself, i.e. to get the newest technologies of processing personal data that meet requirements of the newest technology standards and personal data protection according to this Regulation. The controller is not obliged to implement to the product "privacy by design", this relates only to industrial producers.

Other comments and suggestions to this article that were raised by the delegations at the meetings, we insist on.

Article 24

In this Article of the Regulation proposal we consider it necessary to define that the arrangement about the relation modification among more controllers should be in written and concerned data subject should be adequately informed about adopted rules and procedures. In this case joint and several liabilities will apply to joint controllers and therefore the scheme of application of the data subject rights has to be elaborate and announced to the data subjects, it has to be published in appropriate way. If the data subject addresses a petition to the one of the controllers for the information, rectification, blocking or erasure of data, this asked controller, by doing this operation, releases the others from this obligation. Such a proceeding will not affect the right to regress.

Article 25

We suggest to reformulate paragraph 2 a) in the way to be clear that the controller established in the third country, and also in the third country which ensures an adequate level of protection, is obliged to appoint his/her representative at least at the territory of one of the Member State of the EU, if he processed personal data by means of processing located or dedicated for data subjects in the EU.

We suggest to reformulate the wording of the Paragraph 2 b) or to omit it, to be clear, that this obligation is binding for all the controllers who are processing personal data according to the Article 3 (2) and also for those, who employ less than 250 employees or taking into account other appropriate criteria, which could be exempted. The number of employee or the frequency of offering goods and services is not an appropriate criterion to state duties for the controllers as for the personal data protection. We have just suggested in our previous opinion to take into account another more appropriate criterion, such as the scope of personal data, the number of data subjects concerned, number of persons authorised to process personal data, risk of data processing, etc. The adequacy of personal data protection in the country where
is the controller established is not sufficient guarantee of his observation the EU legislation
or proper communication with the supervisory authorities and conforms to their decisions.

We suggest reformulating or omitting the wording of the Paragraph 2 c) to be clear, that the duty to nominate a controller´s representative is obligatory for all controllers, who
do the personal data processing, according to the Article 3 Paragraph 2.

In the Paragraph 2 d) it is necessary to precise the term *„only occasionally"* – the point 64 of the Preamble, which explains this term as *"secondary activities"* carried along *"main activities"*, gives the space to avoid this provision.

Article 26

The controller and processor relationship is governed by Article 26 of the Regulation proposal. We agree with the content of the point 62 of the preamble that "*the protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor requires a clear attribution of the responsibilities under this Regulation …*"
All concerned articles of the Regulation related to the controller and processor
(as well as "authorised" processor) are necessary to clarify and supplement in this context. Thus we have the following concerns to the Article in question:

In Article 26 absent a treatment of who, in what period of time and how will inform the data subject about selecting of processor that must be incorporate into this Article.

Article 26(2) further:

1. Point b) is incomplete, it does not provide what kind of confidentiality they are committed to maintain, in the same time it is necessary to consider a substitution of this term by another, for ex. "to secrecy" whereas the word "confidentiality" can arouse a doubt arising from its broad semantic content. In this context it is necessary to amend also the wording of Article 81(1) a) of the Regulation proposal which content this wording by the same way;
2. Point d) is not clear:
    a) What position/role will have this so called permitted (secondary) processor, what does mean permission, what legal consequences he has?
    b) If the secondary processor will conform to Article 26(2) subsequently he will have the right to enlist another (tertiary) processor according to the point b) too and the third one another?
    c) If controller does not sign a contract or other act with a secondary processor whom the secondary processor will account for his action to and who will help to ensure obligation according to Articles 30 to 34
    (Article 26(2) f)) to controller or processor who joined him or he will not have this obligation to anyone?

Article 27

The most important comments and suggestions to this article were already raised at the meetings and we insist on them.

Article 28

We propose to reword Article 28(4) according to above remarks of the Slovak Republic. The Slovak Republic has reservation especially to criterion on number of employees and in its previous opinions the Slovak Republic has proposed other, preferable criterion when determining obligations for controllers.

Moreover, paragraph 4 a) is not specific enough in what entity, which is not subject of an obligation to maintain a documentation, shall define. For this reason we propose following text in paragraph 4 a): *"a) a natural person processing personal data for its own needs within the framework of purely personal or household activities, like keeping a personal directory*
or correspondence,".

If cancelled a general controller's obligation to notify and only risk processing are to be assessed, the exception referred to in Article 28(4) b) of the Regulation proposal concerning the limit of 250 persons when keeping "documentation" is too high. We propose to reduce the limit, possibly consider a cumulative condition proposed in connection with EDPS.

Alternatively, we propose to completely withdrawn paragraph 4.

Article 29

The most important comments and suggestions to this article were already raised at the meetings and we insist on them.

Article 30

We consider as a necessary to supplement "personal measures" in paragraph 1. The controller shall, during the processing of personal data and for the purpose of security, implement not only technological and organisational measures but also personal measures.

Article 31

The Slovak Republic in general welcomes an obligation referred to in Article 31 of the Regulation proposal however express doubt with regard to possibility of its realisation from the part of the obliged subjects. Actually, necessary guarantees absent in the Article that this obligation is also reliably filled. Application of the Article will also increase costs for supervisory authorities which will have to be personally strengthened. From the Article it is not also clear what consequence will have an infringement of the notification obligation till 24 hours because in connection to this obligation the supervisory authority will have the power to consider finances setting, which could be too high. Therefore we consider necessary to modify this Article accordingly.

Article 32

It is desirable to put this Article more exact from the point of the legal certainty. For example, it is not obvious who assesses the likelihood if a breach of personal data protection will adversely affect the privacy of the data subject? Is the controller enough professionally equipped to be able to appreciate oneself ugliness of impact according to paragraph 1? It is not also clear in what delay the controller has to notify this circumstance because the term “without undue delay” is not so sufficient in this direction; further in what delay the controller has an obligation to demonstrate this fact to supervisory authority? Etc. For that reason we require to more specifying directly in the Regulation or immediately applied Article 32(5) and issued an act according to Article 86 simultaneously with the Regulation.

Article 33

The Slovak Republic welcomes the intention of this Article but notifies that it may lead to disproportionate burden for small controllers. It would be suitable to specify the text of the Article so that it will be clear what risk operations of processing are subject to an impact assessment, i.e. define more precisely their profiling - cover the processing of certain, resp. all sensitive personal data and their exhaustive enumeration; cover all, respectively certain monitoring of public places, etc. The wording *”on a large scale”* referred in section 2 b) is not defined in the Regulation proposal, therefore it is difficult to use as a criterion.

Article 34

Considerable Article flexibility and ambiguity of the regulation could mean difficulties for its application in practice. Moreover, Article 34(3) transmits the elaboration of proposal on the supervisory authority in the case when the controller does not present adequately justified processing and impact assessment what can cause multiplication of demands on staff of supervisory authority which cannot be foreseen now. Thus worded provision may in certain circumstances also provide opportunities for its abuse by the controller when he deliberately let his "project" to be finalized by the supervisory authority. We deem it necessary to revise and clearly define the draft of this Article.

Article 35

Slovak republic has already in previous opinions objected against 250 employees criterion and suggested to take into account another, more suitable criterions, which would fit better for setting responsibilities of data controllers.

Pursuant to the proposed Article 35(1) b) the obligation to determine supervisory official should apply on subjects which employ more than 250 people. Among other, this highly set number is not possible to agree with because of these arguments: According to available statistics published on 31 December 2011 by the website of the Statistical office of the Slovak republic concerning the number of controllers in Slovak republic – only around 750 controllers had more than 250 employees of the total approximate number of 612 thousands. Under these conditions and without any monitoring responsibility of national data protection authorities through for example registration of information systems there is a justified doubt concerning legality of processing of personal data and compliance with obligations under proposal for regulation by controllers. In addition, our years of experience show that to determine this obligation through number of all employees may not be correct measure in general. More suitable criterion that should be established is to relate the obligation to persons, which come into contact with personal data (so called entitled person[1], which enactment in the Regulation proposal is completely absent). This approach also enhances security of processing of personal data, as controller and processor would have formal obligation to pre-select and instruct entitled persons which will process personal data and to set their access rights. In this case, the obligation to establish supervising officer could take effect in the number of 10 or 20 entitled persons.

[1] We consider as a necessary to introduce a new term "entitled person" in Article 4, i.e. to define a natural person coming into the contact with personal data within the framework of his/her employment relationship, based on the authorization, election or appointment, who may process personal data only upon instruction of the controller or processor. This requirement is necessary to consider the sensitivity since it is needed institute in personal data protection area and it will significantly impact others articles of the Regulation proposal (see comments to articles 22 and 35-37), for ex. Concerning obligations of the controller and processor, eventually when data protection officer has to be appointed. Introduction of this term and obligation to instruct these entitled persons about their rights and duties when processing personal data and modification of related articles of the Regulation proposal will also help to supervisory authorities during the investigation of individual cases as well as it will be beneficial for controllers and processors who will be able to determine labor responsibility to specific employees when breach their duties according to the Regulation proposal, for ex. unauthorised disclosure of personal data to unauthorised persons.

In Article 35(1) c) of the Regulation proposal it is also needed to clarify the intent in terms of legal certainty and to state more precisely its wording.
In Article number 35(3) of the Regulation proposal it is needed to further clarify the term “entity of public authority or body” for the purposes of this regulation; alternatively replace with another, more suitable definition.
In Article 35(7) of the Regulation proposal it is also needed in terms of legal certainty to define the reasons for withdrawal of the data protection officer; alternatively to let the adjustment of this reasons to member states in a way, in which will the independence of his function be maintained.

Article 36

The Article 36 should clearly identify, that supervising officer is not allowed to have the status of statutory body of controller or person entitled to act on his behalf. The previous experiences show, that this fact is necessary to incorporate directly to the articles of regulation not only in the wording “… data protection officer performs the duties and tasks independently...“. Data protection officer should according to Article 37 section 2 perform his function independently, but given the fact that he may be controllers employee, it is not possible to ensure his full independence taking account of his status. Therefore we suggest reformulating this Article in term of this remark.

Article 37

The most important comments and suggestions to this article were already raised at the meetings and we insist on them.

Article 38 and 39

The Slovak Republic agrees with Articles 38 and 39 wording. However in terms of legal certainty these Articles are needed to be further emendated and specified or issue concurrently with the Regulation executive and delegated acts in compliance with Articles 86 and 87.

FINLAND

Article 28

Drafting suggestion:

Article 28

Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain ***categories of all processing operations under its responsibility. This documentation shall contain the following information:***

(a) the name and contact details of the controller, or any joint controller or processor, and of the ***controller's*** representative, if any;
(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the ***regular*** recipients or ***regular*** categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
(f) where applicable, transfers of ***personal*** data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).

2a. Each processor shall maintain the documentation of all categories of processing activities carried out on behalf of a controller, containing:
(a) the name and contact details of the processor and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;

(b) the name and contact details of the data protection officer, if any;
(c) the categories of processing carried out on behalf of each controller;
(d) where applicable, the categories of transfers of personal data to a third country or an international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards.

3. The controller shall keep the documentation referred to in paragraph 1 and 2 available to anyone. This obligation does not apply where data must remain confidential in accordance with a legal provision.

Upon request, the controller and the processor and, if any, the controller's representative, shall communicate the documentation to the supervisory authority.

Justification:
FI proposes a new 3 rd paragraph. Increasing transparency in the personal data processing was one of the elements introduced in the Commission's proposal for the Data Protection Package. We consider that in an open and democratic society not only the data subject but also the public has the right to know how personal data of individuals are used in the society. Keeping the documentation available for all would enhance the transparency in the data processing and strengthen the trust in the lawfulness data processing. There would be no obligation to pass the documentation to the public, but only to keep it available to those who ask for it. Our national experiences suggest that this would not be an issue.

Removal of paragraph 4(a), 4(b), 5 and 6 appears appropriate.

FI delegation is not in favour of the proposed amendment 4(c). There seems to be a risk that the assessment of whether the fundamental rights and freedoms of the data subject could be affected would be carried out by the controller or the processor. This could increase the risk that this obligation would be neglected.

Furthermore, it seems the controller and the processor are entitled to process personal data when processing is necessary for the purposes of the legitimate interests pursued by a controller based on their own evaluation of whether such legitimate interest exists (Art. 6(1)(f)). Thus the minimum requirement set for the controller would be the necessity to define these legitimate interests in the documentation as required under Article 28(2)(c).

It should also be considered whether the filing of the logging data should be addressed separately in this Article.

Article 29

In the Presidency's documents 16529/12 and 5702/13 it is suggested that article 29 is deleted. FI finds the article 29 unnecessary and as such supports the deletion of it. The Article merely states the obvious obligation of controllers and processors to cooperate with the supervisory authorities and as such, the article seems to be unnecessary.

Article 30

The amendments proposed to article 30 paragraphs 1 and 2 in a document 5702/13 seem appropriate. However, the wording in paragraph 1 might need further consideration in order to make it easier to read.

Articles 31 and 32

FI delegation sees the Presidency proposal (in document 5702/13) to add "taken or proposed to be taken" in Art. 31(3)(e) as an improvement vis-à-vis current text. FI also supports adding paragraph 31(3)(a) in the text. Paragraph 3(d) should also be mentioned in subparagraph 31(3)(a).

Drafting suggestion:

Article 31 ***Notification of a personal data breach to the supervisory authority***

1. In the case of a personal data breach which is likely to ***have a significant adverse effect on the*** data subject**s**, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.
2. **(…)** The processor shall alert and inform the controller immediately after the establishment of a personal data breach.
3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
(c) (…) ;
(d) describe the consequences of the personal data breach ***likely to occur***;
(e) describe the measures **taken or proposed to be taken** by the controller to address the personal data breach; and
(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

3a. Where it is not possible to provide the information referred to in **paragraphs** ***3(d) and*** **3** (f) within the time period laid down in paragraph 1, the controller shall provide this information without undue **further** delay **(…)**.

4. The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

[5. 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 establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

Justification:
The personal data breach has not been defined in this Article. It follows that in accordance with the current formulation even minor data breaches should be notified. And furthermore, in case of a failure, there could be administrative sanctions up to 1 000 000 euros. As such, it seems appropriate to frame the notification requirement by adding some further qualifications to it. Proposed formulation has been inspired by the formulation of profiling Article 20(1).

As regards the proposed modification in Article 31(3)(d), it seems unreasonable to require the controller to describe the consequences and this would probably not always be possible either. Therefore FI proposes to add little margin to this requirement by adding "likely to occur" in the end and moving (d)-point under 3(a). It also appears disproportionate to require that such information would always be delivered in 72 hours.

Article 32, as earlier about the definition of the data breach.

Drafting suggestion (Art. 32(4)):

4. Supervisory authority may require the controller to fulfil his obligation to communicate the personal data breach to the data subject.

Or alternatively this question could be addressed in article 52.

Articles 33 and 34

Both Articles 33 and 34 are in essential role in the risk-based approach. The Presidency has also proposed some quite significant changes in these articles to be debated in the working party. As such, these articles need to be further considered once the discussion of the risk-based approach in the working party has been concluded.

Deleting Article 33(4) seems appropriate.

Replacing the Article 34(1) to Article 42(6) seems appropriate.

Article 35

Drafting suggestion:

9. The controller or the processor shall make available the name and contact details of the data protection officer to the public and communicate them to the supervisory authority [upon request..]

Justification

As a general remark, FI is not convinced that such a comprehensive data protection officer institution is necessary. According to some impact assessments this obligation also contains significant additional costs. Also, the obligation to designate the data protection officer seems to add administrative burden. Furthermore, it still needs to be examined thoroughly what kind of incentives could be offered in return.

Furthermore, the requirement to designate data protection officer always when the processing is carried out by public authority or body seems rather excessive. Also, the criterion based on the number of employees for the appointment of the data protection officer might not be the most appropriate one.

As regards the modifications made in document 5702/13; the requirement to make the contact details available for public should not be removed. In accordance with Article 35(10) the data subject has the right to contact data protection officer and as such, to carry out this right, the data subject should be entitled to this information.

Article 36

Presidency has proposed in document 5702/13 to move Art. 35(6) to Art. 36(4). The replacement of this paragraph as suggested seems appropriate.

The modification in Article 36(2) “acts in an independent manner with respect to his or her duties and tasks” is an improvement in respect to the original text.

Drafting suggestion:

Article 36

***Position of the data protection officer*121**

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.
2. The controller or the processor shall support the data protection officer in performing the tasks ***by providing appropriate means to carry out the duties and tasks referred to in Article 37.***

Article 37

The modifications proposed in Art. 37 lead to less prescriptive regulation and as such, FI can support these changes.

Article 38

In general FI sees strengthening the application of Codes of Conduct positively.

Article 39

Last sentence in Article 39(1) would better suit in recitals.

Article 39

Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

UNITED KINGDOM

General Comments:

We welcome the opportunity, provided by the Presidency of the Council, to make general comments and suggested textual amendments on Articles 28-39 of the proposed Regulation. At this stage, we would want to place a general scrutiny reserve on these Articles as there are a number of cross-cutting provisions that interact with later Articles and we would want to consider the package as a whole before reaching a definitive view on all the issues contained within these Articles.

We are providing written comments based on the Commission's proposals, but we have also considered the Presidency paper on Chapter IV. We would like to thank the Presidency for this paper.

With regards to Article 28-39 the UK is proposing the adoption of a risk-based model for the processing of personal data. This would provide data controllers with the required flexibility to assess the risk involved in each processing operation and to take the appropriate measures to ensure the protection of personal data. In addition, we are proposing an increased use of guidance and codes of conduct. A significant advantage of this approach is that it can be quickly updated to take account of new processing techniques, whilst preserving the technological neutrality of the legislation. This is an important principle.

These comments are without prejudice to the UK overarching position that a Directive is the more appropriate form of instrument for this dossier – for reasons we have already articulated.

Article 28 - documentation

Main points

The controller must already be able to demonstrate compliance with the Regulation (see Article 5(f)). **This article is therefore unnecessary duplication and not required**, and would hinder achieving common standards.

In any event, the controller, supervised by appropriate supervisory authority, should be able to evaluate the level and types of risk arising from processing. This cannot be prescribed in a Regulation. **We therefore strongly welcome the Presidency's proposed changes to Art 28(4)**, which we think merit serious consideration.

We also think guidance could – and should – be produced by the supervisory authority or the EDPB, under Article 38. This is an operational function requiring specialist regulatory expertise, and not one for further legislation. **We therefore also agree with the Presidency suggestion that the delegated and implementing acts should be omitted**. We invite the Commission to explain why, if the obligations arising under paragraph 2 are clear enough, standard forms for reporting are needed at all. We think they are not. This is a matter for supervisory authorities in ensuring compliance in general.

This article should not apply to processors at all. The processor processes data on behalf of the controller (Article 4(6)). The controller delegates functions to the processor, but is still liable for the processing under Article 5(f). Related duties on processors should appear (if anywhere) in Article 26. For similar reasons, it is not appropriate to make reference to the representative here.

In Article 28(2)(f), we propose omitting the words from "and" to the end. This is important. This would currently – and we think inadvertently – include a great deal of documentation, and be entirely disproportionate to any risks. Any such reporting requirements should in any event be captured under Article 44.

Other general comments

Omitting the processor from this article illuminates some problems with how the Regulation shares responsibilities out. We strongly agree with the Presidency that the responsibilities of both controller and processor need more careful consideration generally. This is important, too, in Articles 24 and 26. We will return to it there. We will do the same in relation to representatives at Article 25.

This clarification is needed, in particular, to accommodate cloud computing and other technological developments.

Other comments on details

"Documentation" is not technology neutral. It could preclude controllers using innovative means of compliance. We suggest "record" instead.

Article 28(2)(c) duplicates Article 6(1)(f) and is therefore not needed.

We agree with the Presidency's suggestion on Article 28(2)(e), that the words "including the controllers" to the end should be removed. The first controller who is carrying out a task under Article 28 will not necessarily have full details of how another controller is processing the relevant data.

We agree with the Presidency's suggestion of deleting Article 28(2)(h).

Article 29 – cooperation with the supervisory authority

We agree with the Presidency's suggestion of deleting Article 29.

Article 30 – security and confidentiality of processing

Main points

Security is the key to ensuring that personal data are properly protected. **We therefore propose that ensuring appropriate security should be one of the principles set out in Article 5**. Article 30 would therefore specify how the principle should be applied.

Article 5 would therefore include, between (e) and (f):

> "(ee) protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Controllers, supervised by the relevant supervisory authority, should be responsible for ensuring an appropriate level of security. The appropriate level of security should be determined according to the nature of the data and the harm which might result from unauthorised or unlawful processing or loss, destruction or damage to the data, taking into account the state of the art and the costs of implementation.

In complying with the principle of security the controller could be required to consider any relevant guidance under Article 38. This guidance should be issued by the supervisory authority or the EDPB, as appropriate.

The first part of Article 30 would then read as follows:

> **"1. Having regard to the state of technological development and the cost of implementation, a controller must implement appropriate technical and organisational measures to ensure a level of security in relation to the processing of personal data that is appropriate to:**
>
> **(a) the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned in Article 5(ee), and**
>
> **(b) the nature and scope of the data to be processed.**
>
> **2. In complying with the principle as set out at Article 5(ee), a controller must consider any relevant guidance drawn up by the supervisory authority under Article 38."**

Other general comments

We agree with Presidency's suggestion that paragraphs 3 and 4 should be deleted. The appropriate use of technical and organisational measures to ensure security of processing is an operational function requiring specialist regulatory expertise, and not one for further legislation.

We therefore also agree with the Presidency suggestion that the delegated and implementing acts should be omitted. A significant advantage with using guidance is that it can be quickly updated to take account of new processing techniques, whilst preserving the technological neutrality of the legislation. This is an important principle.

We would like to consider the use of pseudonymous data (as mentioned in the Presidency redraft at paragraph (1) further, and will return to this when we revisit the definition of personal data).

The Presidency has introduced an obligation of confidentiality into paragraph 30. We consider that confidentiality is important, but not as important as security. It is also different from security. We think this could be dealt with at Article 26, and elsewhere. Further, confidentiality is not an absolute obligation. We would like to consider how this instrument can reflect this.

Article 31 – notification of a personal data breach to the supervisory authority

Main points

This Article does not respect the privilege against self-incrimination recognised under the ECHR. The following text would resolve this:

> **"A person shall not be required by Article 31 or Article 32 to furnish the supervisory authority with any information if doing so would, by revealing evidence of the commission of any offence, expose him to proceedings for that offence."**

The definition of personal data breach at Article 4(9) is problematic because the unlawful processing of personal data will not necessarily be preceded by a breach of security. Therefore, Article 4(9) should be amended to reflect this.

We agree that the controller should only notify the supervisory authority where the controller considers that there is a **"significant risk that the personal data breach will adversely affect the rights and freedoms of data subjects".**

In making that assessment the controller should be required have regard to factors including the nature of the data; whether the breach appears to be likely to cause substantial damage or substantial distress to the data subject or is otherwise likely to significantly prejudice the rights and freedoms of the data subject and the degree to which those risks are mitigated by the security measures which the controller has taken pursuant to Article 30.

The supervisory authority or the EDPB should provide guidance under Article 38 on the particular circumstances in which notification to the supervisory authority should take place. Further, the level of detail and the specific information required when a controller notifies the supervisory authority of the data breach should be contained in guidance. **The supervisory authority is in the best position to judge the level of detail and particulars which are needed to deal with the breach as effectively as possible.**

Detailed comments

We agree that the supervisory authority should be notified "without undue delay". However, we are not in favour of specifying a timeframe.

We consider that Article 31(2) should be moved to Article 26 as the obligations of the processor are to the controller and not the supervisory authority.

The approach set out above would enable the deletion of paragraphs 3-6. The content of the notification is a matter which the supervisory authority and, if appropriate, the EDPB are best placed to determine. This is an operational matter. Further legislation is not the answer here, not least because as technology changes so will the risks to personal data. Guidance is the best way to ensure that the steps taken deal swiftly and efficiently with emerging threats.

Article 32 – communication of a personal data breach to the data subject

Main points

We think that a data breach should only be notified to the data subject where the controller has concluded that the breach is sufficiently serious under Article 31.

The factors which the controller should be required to consider in doing so include whether the data subject or third party might be able to take steps to minimise adverse consequences, such as financial loss, identity theft, reputational damage or any foreseeable security risk. The controller should be required to consider any guidance issued by the supervisory authority under Article 38, or by the EDPB, as appropriate.

The precise information which the controller should give the data subject or the third party should be set out in guidance from the supervisory authority or the EDPB. Again, this is an operational matter and the relevant authorities will be in the best position to judge what information should be communicated and the manner in which it should be communicated, so as to ensure that the relevant adverse consequences are minimised.

Detailed comments

We welcome the Presidency's insertion of paragraph 3. However, we think that the extent to which appropriate security measures have been taken should apply to the controller's consideration of whether the obligation to notify the supervisory authority under Article 31 has arisen. We have therefore included this as one of the factors for the controller to consider at Article 31.

We agree with the Presidency that paragraphs 5 and 6 should be deleted: these matters should not be the subject of further legislation, but should instead be set out in guidance under Article 38. This ensures that the legislation remains up to date and that the body with operational expertise is able to operate as swiftly and effectively as possible to assist when a serious situation arises.

Article 33 – data protection impact assessment

Main points

We agree in principle that there are circumstances in which conducting a data protection impact assessment (DPIA) would be beneficial. However, controllers are already subject to the substantive obligations in the Regulation. Therefore the additional obligation to complete a DPIA needs to be properly justified, proportionate and clear.

To be of any value, we consider that this article needs to address two issues: the approach of the controller in assessing the **level** of risk; and the **categories of processing** which give rise to risk. We consider that a clear, closed list of categories of processing is helpful and we support the presidency's approach of having a defined list. However, once the controller has ascertained that the processing in question falls within the list, Article 33 should assist in helping the controller to come to a view on the precise level of risk which this particular processing gives rise to.

We suggest that the following approach would be helpful in assessing the level of risk, in place of the current paragraph (1):

> **"A controller who intends to begin processing personal data by an operation described in paragraph (2) of this Article must, before that processing begins, assess the potential impact of that processing on the fundamental rights and freedoms of data subjects and any other person likely to be affected by it. In doing so, the controller must have regard to the nature, scope and purposes of the intended processing. That assessment must describe the intended operations and must:**
>
> **(a) assess the likelihood of the processing operation giving rise to harm to the fundamental rights and freedoms of data subjects or any other person, and the seriousness of any such harm;**
>
> **(b) explain the measures the controller intends to take to mitigate the chance of that harm or its seriousness, including the security measures and other safeguards and mechanisms the controller intends to put in place to ensure protection of personal data in accordance with this Regulation."**

Detailed comments

The list in paragraph (2) needs to be technology neutral. At 2(c) we consider that the words "optic-electronic devices (video surveillance)" should be deleted. The word "automated" should instead be inserted before "monitoring".

We welcome the inclusion of the new paragraph 2a in the Presidency's paper to provide for national supervisory authorities to make public a list of the kind of processing which could be subject to DPIAs, provided that the completion of a DPIA is not mandatory in those cases. We see a role for the EDPB here in achieving harmonisation of approach.

The inclusion of this wording renders the delegated and implementing acts in the original paragraphs (6) and (7) unnecessary.

We would welcome an explanation of the Presidency's paragraph 1a. In our view, a blanket exemption from DPIAs where the data controller has employed a DPO does not take proper account of the need to assess and deal with risks in a proportionate way.

We agree with the Presidency's suggestion to delete paragraph 4.

At paragraph (5) we consider that there should also be a reference to processing under Article 6(1)(e) of the Regulation.

Article 34 – prior authorisation and consultation

Main points

The trigger for prior notification and consultation (notification alone under the Presidency's drafting) combines (i) the fact that an impact assessment has been done with (ii) the conclusion that assessment shows it is likely that there is a "high degree" of a "specific risk".

Controllers would be subject to the general provisions of the Regulation whether or not Articles 33 and 34 apply. Those are therefore additional controls and need separate justification. They need to be proportionate to the actual risks, and deliverable in practice. It has to be very clear when they apply, and what their effect is.

We **agree** that there are cases where the risks of a particular processing operation are such that a controller should consult the supervisory authority before deciding whether to carry it out. We also agree that (if there is to be one) any data impact assessment should be taken into account in such cases.

However, we are concerned that the Article as drafted does not make clear what those cases are. In particular, while Article 33 would address "specific risks", we do not understand the phrase "likely to present a high degree", or how these two ideas relate.

We think there is a solution that will find general approval, and one confirmed by the Presidency's drafting in relation to paragraph 3 (which we welcome). We think the factors listed in paragraph (3) should also inform paragraph (1). The general purpose is the same; the drafting should be too. With that in mind, we propose the following alternative for paragraph 1:

> **"1. Where an impact assessment has been undertaken in accordance with Article 33, the controller must consult the supervisory authority in accordance with this Article if, despite the measures envisaged in the impact assessment to ensure protection of personal data, the controller considers that it is likely that the intended processing would result in serious harm to fundamental rights and freedoms of data subjects.**
>
> **1a. In making that assessment, the controller must have regard to factors including: the nature, scope and purposes of the intended processing; the measures envisaged in the impact assessment to address those risks; the state of the art and the costs of implementation."**

Detailed comments

We agree with the Presidency's suggestion of deleting Article 34(1) and moving it to Article 42(6). We will consider it when we provide comments on Chapter V.

We agree with the Presidency's suggestion to delete paragraphs 4 and 5.

Our approach as set out above renders paragraphs 8 and 9 superfluous.

Article 35 – designation of the data protection officer Main points

We agree that there are cases in which it is likely that a data protection officer should be appointed to enable a controller or processer to comply with the Regulation, and to demonstrate compliance to the satisfaction of the relevant supervisory authority, in a cost-effective way. We are therefore persuaded that there is in principle a place in the Regulation for Articles 35 to 37.

But we do not accept that this will be necessary in all cases referred to in the Commission proposal, even if amended in line with the Presidency proposals. It is essential to ensure that the risks arising from processing are effectively considered; it is equally important to respect proportionality and cost-effectiveness. This is particularly because these Articles would give rise to administrative requirements over and above the substantive requirements of the Regulation – substantive requirements that will continue apply in any event. Appointment of a specific individual to be a data protection officer is *one* way of helping to comply with the Regulation, it is not the *only* way.

In our view, it is the controller or processor who should bear the first and main duty to consider appointing a data protection officer. Member States themselves, in accordance with their domestic law and regulatory practice, should also be able to decide to require the appointment of data protection officers in all cases, or in those giving rise to particular risks.

We therefore propose:

(i) in Article 35(1), inserting "consider whether to" before "designate";

(ii) a new paragraph 1a:

> **"In considering whether to appoint a data protection officer, a controller or processor must have regard to factors including: the nature, scope and purposes of the processing; the risks for the fundamental rights and freedoms of data subjects that may arise from it; the other measures it proposes to take in order to comply with this Regulation; and cost-effectiveness."**

(iii) **a new paragraph 1b:**

"Member States may provide in national law for controllers or processors to be required to appoint a data protection officer for the purposes of this Regulation. In doing so, Member States must at least consider the factors referred to in paragraph 1a. Any such measures shall be notified to the European Commission."

Detailed comments

We agree with the Presidency's suggestions on paragraphs 2, 3, 4, 9 and 10.

We consider that paragraphs 5 and 7 and 8 should be deleted. Paragraphs 7 and 8 interfere with Member State law on employment. We appreciate the efforts which the Presidency has made to avoid this, but we do not consider that this goes far enough. Paragraph 5 is unnecessary. If the tasks of the DPO and the obligations on the controller are clear, the DPO's employment terms should be a matter for the controller to decide.

Our suggested amendments to paragraph 1 and 5 remove the need for a delegated act.

Article 36 – position of the data protection officer

As set out above, the specificities of how the position of DPO is to be administered should be for the data controller to decide. In particular, we do not think that it is necessary to stipulate the management structures and to whom the DPO would report. For example, the requirement that the DPO should report directly to the "highest level of management" suggests that the DPO of a multinational bank would need to report to its CEO. We think this is impractical and unrealistic.

Article 37 – tasks of the data protection officer

We think that this Article is superfluous: it is unnecessary to set out the functions of the DPO. Alternatively their function could be defined in Article 4, but our view is that further elaboration is not necessary.

Article 38 – codes of conduct

We support this article, and welcome the preparation of codes of conduct. We think they are a very useful way of keeping the instrument up to date and sufficiently flexible to deal with new technologies or threats, and ensuring an appropriate level of harmonisation. They could also help controllers to understand how to apply the principles and concepts set out in the instrument apply to emerging ways of processing data.

Detailed Comments

We welcome the Presidency's specific reference to SMEs.

We would seek an amendment to paragraph 2 to clarify that it is the processing the code relates to that needs to be in compliance with the proposed Regulation, rather than the code itself.

Article 39 – certification

We support this article and the idea of certification. We think that professional bodies could be included in paragraph (1) and could also have a role in encouraging the establishment of certification mechanisms and of seals and marks

We agree that the development of seals and marks and other certification mechanisms should be industry-led and subject, if necessary, to the supervision of the supervisory authority, or the EDPB.

The use of further legislation as envisaged at paragraph (2) would shift the emphasis away from industry and regulator-led solutions suggested at paragraph (1). This is undesirable because the operational expertise of industry and the regulator would ensure that data protection systems are practical, up-to date and sufficiently flexible to deal with new technology and new data protection challenges. For similar reasons, we favour the deletion of paragraph 3.

NORWAY

ARTICLE 35: DESIGNATION OF THE DATA PROTECTION OFFICER

We believe that the appointment of a data protection officer can be useful in many cases, and we support the inclusion of an article on this in the regulation. We think that the system should be mandatory only for public authorities who process sensitive data extensively.

We are concerned that article 35 paragraph 7 will interfere with national labour law, and we think it should be rephrased or deleted.