Council of the European Union

Brussels, 31 July 2014
(OR. en)

12267/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 107
JAI 625
MI 574
DRS 102
DAPIX 107
FREMP 146
COMIX 395
CODEC 1671

NOTE

From:	General Secretariat of the Council
To:	Delegations
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) - Risk based approach

Delegations will find below comments regarding risk based approach.

TABLE OF CONTENT

BELGIUM	**3**
CZECH REPUBLIC	**5**
ESTONIA	**9**
IRELAND	**20**
SPAIN	**23**
FRANCE	**26**
CROATIA	**33**
HUNGARY	**34**
THE NETHERLANDS	**38**
AUSTRIA	**54**
POLAND	**60**
ROMANIA	**62**
SLOVAK REPUBLIC	**63**

BELGIUM

Risk based approach

BE is in favour of the risk based approach in order to reduce the unnecessary administrative burden.

Concerning the changes proposed by the Presidency:

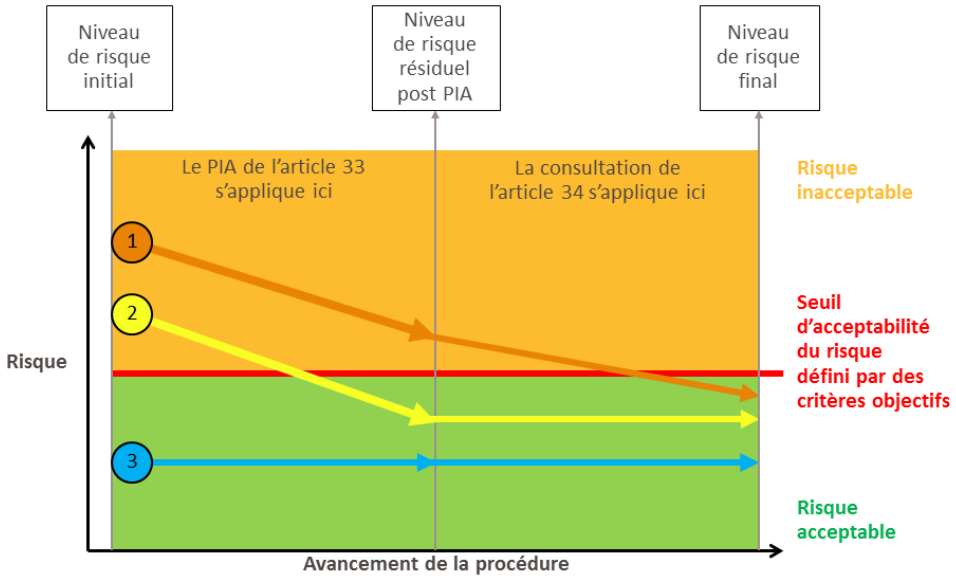
- Point 9, page 3 (art. 22 and recitals 60): BE has a scrutiny reservation on that point. We aren't totally convinced that a definition of low risk could improve the legal certainty. It could be better to talk about acceptable risk or inacceptable risk.

- Point 10, page 3 (Art. 26 §2): BE thinks that the article 26§2 should remain like it is now. It ensure a legal certainty which is necessary concerning the relationship between processors and controllers. It is particularly relevant in a context of cloud computing.

- Point 11, page3 (art. 30): BE is ok with the addition proposed by the presidency.

- Point 12, page 4 (Data breach): BE support the current version of the text. Concerning the recitals, we cannot see the added value of the recital 68 compared to recitals 67 et 68a. The end of the recital 68a should be changed because the reference to the "pseudonymous data" is incorrect. The pseudonymisation of the data doesn't render the data unintelligible.

– Point 13, page 4 (Art. 33): You'll find below (in French, sorry) a schematic explanation on the PIA in link with the concept of acceptable risk and inacceptable risk. This schema helps to understand the logic that could be put in place in article 33 and 34.



Cas 1: risque initial inacceptable >> PIA >> mesures de gestion de risque >> niveau de risque résiduel diminué mais toujours inacceptable >> consultation >> mesures complémentaires >> risque final acceptable

Cas 2: risque initial inacceptable >> PIA >> mesures de gestion de risque >> niveau de risque résiduel désormais acceptable >> pas de consultation nécessaire.

Cas 3: risque acceptable dès le départ >> ni PIA, ni consultation nécessaire

– Point 14, page 4 (Art. 34): BE is in favour of the option c). BE thinks that the options a) and b) are synonymous of a prior authorisation.

– Points 15-16, page 5 (Art. 38 ,38a, 39, 39a): Concerning both codes of conduct and certification, BE thinks that the national DPA's should keep their powers. Moreover, BE thinks that it is very important to foresee a list of criteria that the certification body should use when assessing the controller or processor.

CZECH REPUBLIC

Article 22 paragraph 1

This paragraph should read:

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

Bold text taken from recital 60 to better convey that risk has two components – the probability of harm and the severity of harm. The controller (and DPAs) would then assess both components in particular cases. No definition of risk (low, normal) is provided but the text would not prevent the Regulation to provide particular definitions of low or high risks, if necessary.

Article 26 paragraph 2

CZ believes that qualifying this provision with the words "where relevant" results in too much of legal uncertainty. In the spirit of compromise, CZ supports the insertion of low-risk situations as follows:

~~The~~ ***Unless the risks for the rights and freedoms of data subjects are unlikely and low, the*** carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects (…)and stipulating, in particular that the processor shall:

Article 33 paragraph 2 and recital 71

The text should read:

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

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

(b) processing of **[special categories of personal data under Article 9(1), ~~data on children,~~ biometric data]** or **data on** criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals **(…)**[**and *which is contrary to* legitimate expectations of the data subject ~~are not met~~, for example owing to the context of the processing operation]**;

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

(d) **(…)**;

(e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects[**, or because *it is more difficult for data subjects to exercise their rights under this Regulation* ~~they prevent data subjects from exercising a right or using a service or a contract,~~ or because they are carried out systematically on a large scale]**.

On b): CZ does not agree that processing of data on children always involves high risks. Processing of data on vulnerable children either happens based on Article 8, which should decrease the risk significantly, or on the basis of contract (again) or law.

CZ further believes that if legitimate expectations should be considered in relation to risks, we should focus on processing where the legitimate expectations of the data subject (and therefore his/her further behaviour) are contrary to the real processing. This would make the application of this rule easier as well – it would be necessary to consider only how much the expectations were divergent from the reality rather than establish what the expectations exactly were and whether they had been met (in sufficient degree).

*On c) and e): CZ notes that very uncertain term "**on a large scale**" is repeated. IT PRES lists certain examples for (e) (document 11481/14, point 13), such as "doctors, hospitals, attorneys and border agencies". This illustrates the problem. If a doctor is presumed to process personal data on the same "large" scale as a hospital, if a lawyer is comparable to a border agency (which lawyer processes data on millions of individuals?) where exactly "large scale" begins? It is not even clear whether an enterprise with hundred? or thousand? employees would be always in high risk. Therefore CZ would plead to **either clarify this wording or to have at least more focused examples or interpretations provided in a recital**.*

On e): CZ proposes to get the wording in line with recital 71 as far as exercise of rights is concerned, and to refer specifically to rights according to this Regulation.

CZ considers the language on "preventing from using a service or a contract" to be way too vague – every service which is e.g. unavailable to children or in certain regions would be covered. CZ believes that such cases should be regulated in different areas of law (protection of morals, children, consumers, competition etc.).

*CZ further notes that **recital 71** is not fully compatible with the **Presidency proposal** on Article 33 - e.g. the wording on "secrecy", "new technology" does not correspond to the actual text of Article 33. Therefore, it should be **amended correspondingly**.*

Article 34 – the Presidency text on p. 4, paragraph 14

*CZ **does not support the options** listed by the Presidency under (a) and (b). Option (a) would demotivate controllers that would wish or need to start with data processing as soon as possible and could also put undue strain on DPAs. Option (b) would again motivate the controller to avoid any dialogue with the DPA for fear that the processing would be prohibited on "hypothetical" basis even if no data subject would find it objectionable in practice. CZ prefers strong powers of the DPA to solve actual rather than hypothetical situations. CZ understands that (c) is already covered by Article 79a(3)(i) of the document 11028/14.*

Article 34 paragraph 7

The paragraph should read:

Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure adopted by a national parliament or of a regulatory measure based on such a legislative measure which provide for the processing of personal data ***unless they are likely to present only low risks for the rights and freedoms of data subjects***(…).

A recital should then clarify that "non-standard" preparation of legislative proposals refers to private members' bills or special rules for law-making during war time or similar conditions.

The second addition is meant to uphold risk-based approach and to exclude simple data processing mandated by various rules made by municipalities etc. from consultation duty (which might either paralyze municipalities or DPAs)

ESTONIA

I. Risk based approach

(1) General comments regarding the risk based approach as a concept

Firstly we would like to point out that we support the risk-based approach in the Regulation, because it will help to reduce the administrative burden, especially for SMEs. Furthermore, we believe that the Regulation contains more or less a balanced risk-based approach. However, on one side, we would prefer that the risk-based approach would be included also in articles 14 and 14a (information to be provided to the data subject), article art 57 (consistency mechanism) and article 26 to lower the administrative burden even more. On the other side, we are ready to look into other possibilities for reducing administrative burden in the before-mentioned articles (e.g. adding to articles 14 and 14a the condition that some or most of the information should be provided on request). Furthermore, recital 63a (explaining article 26) actually already uses the reference to risks. Namely risks have to be taken into account for drafting the content of the contract or other legal act between the controller and the processor. To sum up, we believe that current outcome is quite balanced, but there is always a possibility to prove, especially in the before-mentioned articles.
In general, as mentioned in the working parties, we would like to have more consistent risk-based approach, which would apply to the regulation as a concept. Therefore, we have suggested to have a general risk definition (possibly including low and high risk) in the general provisions of the Regulation. We believe that delegations expressed different views in the working party, but some agreed that there is a need to define risk as a notion. We believe it is necessary as a legislator to give some broad concept of the before mentioned terms to make the implementation and understanding of the risk-based approach more clear for the data protection supervisory authorities (hereinafter DPA).

Furthermore, it would be helpful to have a more consistent and systematic terminology. Currently we are using different notions (e.g. risks, specific risks, high risks, high degree of specific risks, severely affect), which might affect the overall concept and interpretation of specific paragraphs. In our opinion, in the last version of the text, there are currently four different levels or notions of risk:

1. Risk: We understand that risks are all situations that might prejudice the interest of a data subject, i.e. cause physical, material or moral harm. Recital 60 gives a list of examples, what could be seen as situations, which present any kind of risk. The notion is mentioned in several articles (e.g. art 22, 23, 30). However, there is less examples mentioned in article 30(1a) than in recital 60. Therefore, in our view, it might be inconsistent. We understand that article 30 (security of processing) needs more specific examples than the general risk in article 22 and recital 60. However, it might be necessary to have a better link to the general risk notion in recital 60.
2. Specific risks: In our view, specific risks are a more severe level of risk situations (but not the highest nor the lowest), which will require a higher protection than low risk situations. The notion is mentioned in articles 25 and 28 as well as recitals 63 and 65. Currently the text does not contain a list of examples for situations that are considered as presenting a specific risk for the rights and freedoms of the data subjects.
3. High risks: We are not sure of the necessity to replace the notion "*specific risks*" to "*high risks*" in article 33. We believe that it might actually make the whole risk-based approach confusing. Namely, beforehand there was a connection between article 34 and 33, because article 34 mentions high degree of specific risks. This meant that if the processing was likely to present specific risks, then an impact assessment was supposed to be carried out. Furthermore, if the assessment resulted in the conclusion that the processing creates a high degree of specific risks, then the DPA had to be consulted. Therefore, there was a two-step obligation. However currently, it seems that there is no connection between article 33 and 34, unless "*high risks*" means the same as "*specific risks*".
4. High degree of specific risks = severely affect: we believe that the notions of "*high degree of specific risk*" and "*severely affect*" conclude the same risk level, i.e. the highest risk, which might cause severe physical, material or moral harm. Therefore, this level needs the highest protection (i.e. fulfilling the obligations mentioned in articles 31, 32 and 34).

To sum up, our purpose is not to define the risk in a closed manner or bring an exhaustive list of examples. We understand that this is impossible due to the ongoing changes in different fields. However, there should be a broad definition with different examples (as provided already in the text) and they should create a coherent and clear system. In our opinion, the current concept might be, to some extent, too complex, i.e. it might be hard to understand, which level and which examples are applicable to which obligation.

Hence, we suggest the following minor changes to the wording without too much changing the currently used notions nor changing the structure of the text (*changes are made in bold, underlined and red; on the basis of the last wording in document No. 11481/14*):

60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. **These risks are situations, where based on an objective assessment, it can be deemed sufficiently probable that data processing is likely to prejudice the rights and freedoms of data subjects.**[1] Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage; or
- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed;

---

[1] We believe that this general notion would give a better understanding, what is understood as „*risk situation*" and would make it easier to interpret it through-out the whole Regulation. We would even prefer to have the definition in article 4, but it might be enough to add it only to the recital.

- where processing involves a large amount of personal data and affects a large number of data subjects.

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the **(…)**[2] risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). **In assessing data security risks, consideration should be given, to risks that are presented by data processing, which could lead to physical, material or moral harm, in particular (…)**[3] **to accidental or unauthorised access, destruction, loss, modification or dissemination of personal data.**

[2] We understand that recital 66 explains the obligation set out in article 30, i.e. security of processing. However, the article does not mention „*specific risks*" but „*risks*" in general as this obligation applies in any risk situation.

[3] In our opinion the addition would create a link to the recital 60, which explains the general notion of risk. Therefore, it will clarify that the evaluation of data security risks, should also consider the examples given in recital 60 in addition to the specific examples given in this recital.

67) A personal data breach may, if not addressed in an adequate and timely manner, result in severe **physical**[4], material or moral harm to individuals such as **substantial** loss of control over their personal data or **significant (…)**limitation of **(…)** their rights, **unlawful or arbitrary** discrimination, **substantial** identity theft or fraud, **significant** financial loss, **significant** damage of reputation, **significant** loss of confidentiality of data protected by professional secrecy or any other **significant** economic or social disadvantage to the individual concerned.[5] **Such severe harm or a high degree of specific risk is presented by certain type of data processing and certain extent and frequency of processing, which may result in a realisation of extensive damage or disproportionate harm to rights and freedoms of data subject.**[6] Therefore, as soon as the controller becomes aware that (…). a personal data breach has occurred, **which may result in severe physical, material or moral harm**[7]the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals **whose personal rights and freedoms** could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. **(…)**. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects.

---

4 In recital 60, where the general risk notion is mentioned, we use the words „*physical, material or moral harm*" to explain it Therefore, to keep the consistency, we should use the adjective „*physical*" also in this recital or alternatively, delete the adjective from recital 60.

5 The examples listed here are to some extent the same as in recital 60, which explains the general risk notion. Therefore, we believe it is necessary to clarify, that in this context those examples have to be severe (high degree) or alternatively erase the list from this recital. It has been done to some extent in recital 71. Therefore, we suggest to adjust this recital accordingly.

6 We believe that there is a need to have a general definition of the notion „*high degree of specific risks*" and link it to the notion „*severely affect*" as well as the notion „*specific risks*", which are listed as examples in article 33(2) taking into account the type of data (i.e. sensitive data) as well as the extent/frequency of the processing (i.e. systematic and extensive; on a large scale etc.). We would even prefer to have the definition in article 4, but it might be enough to add it only to the recital.

7 This part of the sentence was erased in the last document, however we wonder, what could be the reasons behind it. Namely, without that part of a sentence, it might be understood, that the controller has to notify the DPA in any breach not just a breach, which might result in severe physical, material or moral harm as stated in article 31 (i.e. this might cause an inconsistency between the recital and the article).

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 need** 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.

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 obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those processing operations which are likely to present **(…) specific**[8] risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes **and context**(…). In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the severity and likelihood of these specific risks, taking into account the nature, scope and purposes of the processing and the sources of the risks, which should include in particular the envisaged measures, safeguards and mechanisms **for mitigating those risks and** for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

---

8 We are not sure of the necessity to replace the notion "*specific risks*" with the notion "*high risks*". We believe that it might actually make the whole risk-based approach confusing. Namely, beforehand there was a connection between article 34 and 33, because article 34 mentions high degree of specific risks. This meant that if the processing was likely to present specific risks, then an impact assessment was supposed to be carried out. Furthermore, if the assessment resulted in the conclusion that the processing creates a high degree of specific risks, then the DPA had to be consulted. Therefore, there was a two-step obligation and we would like to keep it that way, i.e. change it back to "*specific risks*". Furthermore, in this case, this recital and article 33 would also give an indication for articles 25 and 28 (including recitals 63 and 65) as to the meaning of the notion "*specific risks*" mentioned in those articles.

71) Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a high degree of specific risks to the rights and freedoms of data subjects, such as **substantial loss of control over their personal data or significant limitation of (…)**their rights **(…)**,unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of the processing activities.[9] **Such severe harm or a high degree of specific risk is presented by certain type of data processing and certain extent and frequency of processing, which may result in a realisation of extensive damage or disproportionate harm to rights and freedoms of data subject.**[10] The supervisory authority should give advice where the envisaged processing might not be in compliance with this Regulation. The supervisory authority should respond to the request for consultation in a defined period (…). However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its **tasks** and powers laid down in this Regulation. Such consultation should equally take place in the course of the preparation of a legislative or regulatory measure which provide for the processing of personal data(…).

As part of this consultation process, the outcome of a privacy impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate possible risks for the rights and freedoms of data subjects.

---

9 The examples listed here are to some extent the same as in recital 60, which explains the general risk notion. Therefore, we believe it is necessary to clarify, that in this context those examples have to be severe (high degree) or alternatively erase the list from this recital. It has been done to some extent in this recital already by adding the words substantial or significant. However, we suggest to align the first part of the examples to the wording of recitals 60 and 67, as it might be better to understand it.

10 We believe that there is a need to have a general definition of the notion „*high degree of specific risks*“ and link it to the notion „*severely affect*“ as well as the notion „*specific risks*“, which are listed as examples in article 33(2) taking into account the type of data (i.e. sensitive data) as well as the extent/frequency of the processing (i.e. systematic and extensive; on a large scale etc.). We would even prefer to have the definition in article 4, but it might be enough to add it only to the recital.

Article 30

Security of processing

1a (...)[11]

[*Other paragraphs of this article are not changed*]

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 **present high degree of specific risks to (…)** [12] the rights and freedoms of data subjects 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.

[*Other paragraphs of this article are not changed*]

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to **present high degree of specific risks to (…)**[13]the rights and freedoms of the data subject, the controller shall (…)communicate the personal data breach to the data subject without undue delay.

[*Other paragraphs of this article are not changed*]

---

11 We believe it might be sufficient to cover it only in the recital as it has been done for the general risk notion in recital 60 and not in article 22. However, we would accept to keep it also in the article, but in this case the wording of the recital 66 and article 30(1a) should be a bit more coherent. Namely, currently different notions are being used.

12 For the purposes of a more coherent approach, we should use same notions for the same levels. We have understood that the obligations in articles 31, 32 and 34 have to be fulfilled only in cases, where the presented risks are the highest. Therefore, we suggest using the same notions in the before-mentioned articles, which can be interpreted also via the list of specific risks in article 33(2).

13 *Same comment as above.*

Article 33

Data protection impact assessment

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present **specific (…)**[14]risks for the rights and freedoms of data subjects, the controller **(…)**shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…). **(…).**

1a. The controller shall seek the advice of the data protection officer, where applicable.

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

3.

[*Other paragraphs of this article are not changed*]

(2) Answers to specific questions

We believe that there is three different topics raised by the Presidency that we have not yet covered in our interventions nor in the comments above.

Firstly, there were changes made to article 33(2)(b) (as well as recital 71) and article 33(2)(e), which were explained in point 13 of the document No. 11481/14.

Regarding article 33(2)(b), we are not sure, what is exactly meant by "*legitimate expectations are not met*" or "*owing to the context of the processing operations*". Furthermore, the addition to recital 71 might not explain the concept fully. Therefore, we agree with the Presidency's statement that it might affect legal certainty more than the previous text. However, we are of course flexible with the wording, if it would be possible to clarify the new notions. Namely, we also think that the notion "*large scale*" has been currently explained better in recital 71 than the new terminology used.

---

14 We are not sure of the necessity to replace the notion "*specific risks*" with the notion "*high risks*". We believe that it might actually make the whole risk-based approach confusing. Namely, beforehand there was a connection between article 34 and 33, because article 34 mentions high degree of specific risks. This meant that if the processing was likely to present specific risks, then an impact assessment was supposed to be carried out. Furthermore, if the assessment resulted in the conclusion that the processing creates a high degree of specific risks, then the DPA then the DPA had to be consulted. Therefore, there was a two-step obligation and we would like to keep it that way, i.e. change it back to "*specific risks*". Furthermore, in this case, this recital and article 33 would also give an indication for articles 25 and 28 (including recitals 63 and 65) as to the meaning of the notion "*specific risks*" mentioned in those articles.

Regarding the additions to article 33(2)(e), we believe that they should be drafted as examples of "*presenting specific risks for the rights and freedoms of data subjects*". Namely, article 33(2)(e) has been a sub-paragraph, which will make the list non-exhaustive, i.e. the DPA can always interpret more situations as presenting specific risks for the rights and freedoms of the data subject. Therefore, the additions "*because they prevent data subjects from exercising a right or using a service or a contract*" and "*because they are carried out systematically on a large scale*" as alternatives to "*present specific risks for the rights and freedoms of data subjects*" might create systematically a confusion.

In our opinion, the most logical choice would be to draft the new text so, that they would be understood as examples of situations that present specific risks for the rights and freedoms of data subjects. Therefore, the word "*or*" could be replaced by the word "*including*".
Secondly, there was a question raised by the Presidency in point 14 of the document No. 11481/14 regarding some additional instruments for article 34. Namely, should we add the following options to the prior consultation regulation?

a) *Prohibiting processing operations pending the opinion of the data protection authority:*

In our opinion, in case of prior consultation, we should not provide the DPA an instrument, whereas it can prohibit the processing operations pending its own opinion. Namely, it might have a huge negative effect on the enterprises, especially for the reasons that the infringement has not yet been identified. Therefore, it might also go against the main principles of the administrative proceedings, whereas an action should be taken or a specific measure applied only, if there is a clear infringement.

b) *Prohibiting processing operations for which the data protection authority has rendered a negative opinion:*

We agree that if the DPA has rendered a negative opinion there should be an option to prohibit the processing operations. It might be of course already possible via the powers listed in article 53. However, it might cause additional administrative burden for the DPAs, because different procedural rules have to be followed, which might have been already followed during the opinion process (e.g. the right of every person to be heard; obligation to investigate etc.). Therefore, it might be reasonable to add the option to prohibit the processing operations due to a negative opinion already to article 34.

c) *Providing for an administrative sanction in case of failure to consult the data protection authority:*

There is definitely a need to have an administrative sanction in case of failure to consult the data protection authority. However, we do not see the need to add it to article 34 as the administrative sanction is already provided for in article 79a(3)(i) as mentioned also in the Presidency's document.

Thirdly, there was a question raised by the Presidency in point 16 of the document No. 11481/14 regarding article 38 and 39. Namely, the Presidency wanted to know, which role the data protection authorities should play in both mechanisms (code of conducts and certification).

We can support the proposed text by the Presidency. We believe that it is necessary to involve the DPAs in both processes: code of conducts and certification mechanism

IRELAND

These comments are based on the text of chapter IV as set out in document 114/81 of 3 July 2014.

Article 22

Ireland supports the risk-based approach set out in article 22 and recital 60.

The level of actual risk (low; moderate; high) often depends on the context in which the processing takes place and this is very difficult to define in detail.

As regards future risk, the words of US Defence Secretary Rumsfeld in a different context seem appropriate: "*... We also know there are known unknowns; that is to say we know there are some things [risks] we do not know. But there are also unknown unknowns, the ones [risks] we don't know we don't know.*"

Article 23

In paragraph 2, Ireland suggests replacing "not excessive" with "necessary". The current wording "*... only data which are not excessive for each specific purpose ...*" is bad English and unclear. Using the word "necessary" instead would improve the text.

Article 26

Ireland can support the current text of this article but is opposed to the inclusion of any further detail or complexity. Any further changes would risk creating unnecessary and disproportionate burdens and compliance costs in cases of routine controller-processor interactions.

Article 30

In paragraph 1a, insert "appropriate" before "level of security".

Article 31

Ireland strongly supports retention of paragraph 1a. Otherwise, there will be a possibility that supervisory will be overburdened with notification of relatively unimportant breaches, e.g. losses or destruction of mobile phones.

Article 33

Ireland prefers reference to "specific risk" instead of "high risk".

In paragraph 2b, the term "legitimate expectations" should not be used; consider replacing with the following: "except where such processing is reasonably likely to take place in the context of the processing operations". This means that processing of sensitive personal data could be undertaken in hospitals or prisons without an impact assessment because it is reasonably likely that such processing is a normal activity in such contexts.

The intention behind paragraph 3a is unclear, especially the reference to "lawfulness" of processing operations.

Article 34

Ireland has a complete reserve on paragraph 7 because the scope of this obligation has become very general and, therefore, uncertain (there is no recital).

Many legislative measures, mainly legislation, make provision for "the processing of personal data" of a routine or relatively straightforward nature and should not fall within the scope of this provision.

For example, any amendment to the law relating to the registration of land ownership, or tax law, will inevitably require, and permit, the processing of personal data. Our worry is that in the future a legislative measure (e.g. tax law) on which the supervisory authority has not been formally consulted could be declared void by the courts because of the lack of consultation. Earlier versions of the text of paragraph 7 included the words "and which may severely affect categories of data subjects by virtue of the nature, scope or purposes of such processing" but this filter has now been removed. We request the inclusion of this, or similar, wording.

Articles 35 to 37

As agreed at the March 2013 JHA Council, the appointment of a data protection officer must remain optional.

Articles 38 and 38a

We can support the text of these articles as well as the structures and procedures set out in them. Monitoring by the accredited body, which is necessary, is without prejudice to the tasks and powers of the supervisory authorities.

In paragraph 4 of article 38a, the accredited body is given power to suspend or exclude controllers and processors that have infringed the code. This means that the accredited body must have monitoring powers which are separate from those of the supervisory authority. The text of paragraph 1b of article 38 may, therefore, need to be adjusted in order to make this clearer. Perhaps something on the following lines:

> *"1b. Such a code of conduct shall contain mechanisms* ***which enables the body referred to in paragraph 1 of article 38a to monitor compliance with its provisions*** *by the controllers or processors which undertake to apply it, without prejudice etc."*

Articles 39 and 39a

Ireland is opposed to paragraph 2a in article 39, and connected changes in paragraphs 3 and 4, because they undermine the structures and procedures set out in articles 39 and 39a.

The intended tasks of the supervisory authorities in respect of the certification mechanism are set out clearly in article 52.1(gb) (i.e. promotion activity); (gc) (i.e. periodic review), and (ha) (i.e. conduct accreditation of monitoring body). The supervisory authority should not issue certifications unless it is, at the same time, also the accredited body (e.g. the supervisory authority in Schleswig Holstein which already operates such a scheme.

SPAIN

The Spanish delegation welcomes the Presidency´s initiative to discuss the risk-based approach of Chapter IV and the impact of the ECJ judgment regarding the Spain vs Google case on Article 17 of the draft regulation.

Comments on the risk-based approach document

Point 9

Spain has always supported the risk-based approach under the understanding that there is no zero-risk in processing operations. Every processing operation of personal data involves risks, though maybe minimal. Therefore, there must be always a certain number of obligations that should be fulfilled at any rate. This is why Spain would find it useful to introduce a definition of "low risk", linked to a number of minimal obligations. "Low risk" would refer to the inherent minimal risk involved in any processing operation with personal data. From that point, taking into account the specific situations of the processing considered (quantity of personal data processed, processing of special categories of data…), this processing can be considered more risky, and so more obligations should be imposed.

Point 10

We would not support the approach suggested by the Presidency. The controller and the processor will always sign a contract to determine the conditions of the service rendered and the mutual obligations. Article 26.2 merely establishes certain elements related to data protection that must be expressly clarified in the contract´s content, just as there are other elements determined by other laws (object of the contract, duration, liability…). The elements referred to in this article are not excessive, they are the minimal aspects required to clarify the data protection regime.

We should also take into account that the list of elements in Article 26.2 cannot be understood as compulsory in every case. For example: if the service will be rendered directly by the processor, without the intervention of a subprocessor, obviously the contract shall not refer to "respect the conditions for enlisting another processor" (Art. 26.2.d).

In sum, Spain would not be in favor of wording this article in a less prescriptive manner. As a compromise to achieve an agreement in this point, we would prefer introducing the words "where relevant" rather than introducing a risk criterion as suggested in the Presidency´s paper, as we understand that the current wording of Article 26.2 already implies a "where relevant".

Point 12

The Spanish delegation is in general terms satisfied with the approach on data breach notification.

Point 13

Spain would be in favor of introducing the first sentence of the proposal of the Presidency regarding Article 33.2.b) ("special categories of personal data under Article 9(1), data on children, biometric data"), but is opposed to the new wording of the last part of the article ("and legitimate expectations of the data subject are not met, for example owing to the context of the processing operation").
As we understand it, DPIAs are not instruments that legitimate data processing operations. They do not determine *if* the processing can take place, but *how* it should take place. By carrying out an impact assessment, the controller realizes the different risks involved in the processing operation, and can take measures to reduce the risks to the minimal possible. It is an instrument that helps the controller to acquire conscience of the nature and dangers that a certain processing operation might produce.

Therefore, we believe that the fact that a certain processing operation meets the legitimate expectations of the data subject does not imply that, considering the nature of the processed data (sensitive data) and the consequences of this processing operation (decisions on individuals), the processing operation examined does not present certain risks that should be assessed and dealt with.

Additionally, we would appreciate that the Presidency clarifies the new wording of Article 33.2.e): "other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects[**, or because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale]**". For us, it is unclear whether the new circumstance introduced by the Presidency is referred to i) the fact that the competent authority considers that the processing presents specific risks *because* they prevent the data subject from exercising a right, or ii) the fact that the processing prevents data subjects from exercising a right is *itself* (that is to say, with no intervention by the DPA) a circumstance that transforms a risk into a high risk.
We do not oppose to any of the two possible interpretations, but we would appreciate to know which one was the Presidency thinking of when introducing the new text.

Point 16

From our perspective, the Data Protection Authorities should always keep the competence for supervision, although it might be additional to the supervision competences that could be attributed to the specific bodies referred to in Article 38a. This is consistent with the current Spanish law: the specific supervision authorities (the bodies referred to in Art. 38a) verify the compliance with the additional obligations and compromises assumed by the controller in the code of conduct, while the Data Protection Authority supervises the fulfilment of the code of conduct regarding the obligations directly derived by the Law. Excluding in an absolutele way the DPA from playing any role in the supervision of the compliance with a code of conduct would be autoregulation, which is something that is not intended by the Regulation.

As regards to whether we would prefer certifications to be issued by a certification body accredited by the data protection authority or also by the data protection authority itself, Spain is in favor of allowing each Member State to choose between the two possibilities. In the particular case of Spain, our Data Protection Authority is dubious whether it could undertake the burden of developing the certification procedure, especially taking into account that it lacks the particular expertise required by this activity. Nevertheless, Spain understands that other DPAs may be in a position to deal with these procedures and, therefore, we would suggest offering both options so that each Member State can decide which option meets their possibilities.

FRANCE

First, the French authorities would stress that the following comments relate only to the risk-based approach and are without prejudice to our other comments on the substance of the articles in Chapter IV. Those comments will be submitted in due course, when those articles are examined in detail.

We would point out that we support the principle of the risk-based approach in that it gives responsibility to controllers and processors, motivating them to take appropriate measures to address the risks involved in the data processing they carry out, or face having their responsibility called into question.

Our thoughts on the risk-based approach in Chapter IV are centred around **three main horizontal themes**, which are the focus of most of the Presidency's questions and suggestions in the cover note to its working document:

1) **use of the tools and procedures provided for in Chapter IV** (impact assessments, data protection officer, codes of conduct, certification mechanisms) **must not allow controllers or processors to shirk their responsibilities with regard to data processing once they have implemented or set up such mechanisms, as the risks inherent to the processing remain unchanged**.

● For example, we do not support the **use of pseudonymous data** as a means of calibrating controllers' and processors' data protection obligations (see paragraph 5 of the Presidency working document). Pseudonymous data should only be used to demonstrate that the controller or processor has put something in place to reduce the risks involved in the processing (which will otherwise continue to present the same risks), and cannot justify a lighter regime on obligations for the controller or processor. This is also the position of the WP29 (cf. point 10 of the statement of 30 May 2014).

With particular regard to the communication of security breaches to data subjects (Article 32), the French authorities remain concerned that pseudonymisation might exempt the controller or processor from having to effect such communication (cf. recital 60a, which corresponds to point (b) of Article 32(3)). In addition, insofar as Article 31 concerns notification to the supervisory authority of a breach which is likely to severely affect the rights and freedoms of data subjects, we would like this article to be supplemented so as to provide for the response by the supervisory authority. The fact that the text is currently silent on the matter is problematic, particularly in view of the one-stop shop mechanism.

We therefore propose that the following wording be added:

"The supervisory authority shall decide how to respond to the notification, in line with the consistency mechanism for cross-border data processing operations".

● Similarly, we believe that the risk-based approach should under no circumstances result in controllers being exempt from the **documentation requirement**, which is essential both internally for enterprises and for the supervisory authorities in the performance of their duties (cf. point 6 of the statement of 30 May 2014 and footnote 59 in the Presidency document).

● We are also against **the adoption of a code of conduct or the use of certification mechanisms** being taken into account in the context of data processing risk assessment (see paragraph 6 of the Presidency document). Those tools should only be used to reduce the risks presented by data processing, once the risk level has been assessed (in this regard, we would stress that Article 33 on impact assessment states, in paragraph 1, that data processing, "*taking into account the nature, scope or purposes of the processing*", is likely to present high risks, and this will remain the case regardless of the mechanisms or safeguards implemented.

The adoption of a code of conduct must also not reduce controllers' and processors' obligations when assessing the risks presented by data transfers to third countries (see the Presidency's suggestions in paragraph 15 of the working document and in Article 33, new paragraph 3a). In this respect, we believe that our suggestion of introducing a certification mechanism for data transfers to third countries would provide a safer framework for such transfers, particularly in allowing supervision by the European authorities (see point 3) below).

● Similarly, although the **designation of a data protection officer** may help controllers and processors to fulfil their obligations, we believe that it must remain optional and also must not reduce the obligations they have as a result of the risks presented by their processing operations, or diminish data subjects' rights with regard to their personal data.

● We are ultimately against the Presidency's suggestion of adding a **definition of "low risk"** to Article 22 of the proposal for a Regulation (see paragraph 9 of the Presidency document). Low risk must be defined *a contrario*, in relation to high risk. It is therefore this high risk category which should be better defined in the proposal for a Regulation.

In general, the Regulation should expand on the concept of "risk", which is crucial for legal certainty. For instance, the Regulation could include points relating to criteria for assessing risk and the degree of risk. However, insofar as the Regulation cannot go into too much detail, given the complexity of the subject matter and the need to maintain the technological neutrality of this instrument, we believe that it should be up to the EDPB to set out guidelines for all parties.

● We wish to enter a scrutiny reservation on **Article 26 (obligations of the processor)**, and will submit in due course specific comments on the division of responsibilities and the respective obligations of the controller and processor.

● We note that the Presidency's proposals in respect of the **concept of security** (see paragraph 11 of the working document) bear out our approach to the mechanisms provided for in Chapter IV. The risks which arise from accidental or unlawful destruction, loss or alteration of data (etc.) and which must be taken into account when assessing the level of security of data processing must be assessed in order to allow appropriate security measures to be taken. In this respect, the Presidency's proposals regarding the addition of a new paragraph 1a to Article 30 are a step in the right direction.

● Finally, with regard to the Presidency's proposals in respect of **risk assessment criteria** (see paragraph 13 of the working document):

- We basically **support** the Presidency's proposal that the concept of risk should be developed by specifying in Article 33(1) and (2) that the risk must be high.

- However, we have **reservations** about the deletion of "*large scale*" from point (b) of Article 33(2), and await clarification of the concept of "*legitimate expectations*" which the Presidency has proposed instead. We welcome the Presidency's intention in this respect, but more detail is needed on this concept of "legitimate expectations", and the reference to the context of the data processing operation must be clarified. As it stands, the wording is too vague.

- As regards recital 71, which now incorporates this concept of "legitimate expectations", we have **reservations** about the concept of "new technology", which we consider too vague. This concept appears to be unsuitable, insofar as it is not the technology in itself which presents risks but rather the way it is used in data processing.

- Finally, we have **reservations** about the amendments made to point (e) of paragraph 2, insofar as these seem to duplicate other points in that paragraph. Paragraph 2 should therefore be rewritten more coherently. In particular, the concept of "preventing them from exercising a right" seems to be covered already given the very principle of "specific risks for the rights and freedoms of data subjects".

2) The proposal for a Regulation should provide for **strict control of the most high-risk processing operations by making the supervisory authority's opinion binding (Articles 33 and 34)**.

● Provision must be made for a mechanism guaranteeing the persons concerned that if a data processing operation poses high risks for their rights and freedoms and receives a negative opinion from the supervisory authority, it cannot be carried out. Since the opinion is not binding under the current text, a processing operation could be carried out even if deemed by the supervisory authority to pose excessive risks, with no obligation to inform the persons concerned. **This puts the persons concerned directly at risk and decreases the level of protection currently offered by EU law, which provides for an authorisation procedure**.

● Furthermore, the data processing authorisation procedure should also enable the supervisory authority to take responsibility by issuing an opinion on the most high-risk data processing operations, since it will then have to monitor their execution.

● **That opinion should be binding; this is the only way to guarantee that all supervisory authorities concerned will be informed and involved in the authorisation procedure for particularly risky and sensitive data processing operations**. In this regard, we thank the Italian Presidency for its comments in paragraph 14 of its working document. We support the three proposals relating to the prior authorisation procedure in Article 34, as put forward in points (a) (prohibiting processing operations pending the opinion of the data protection authority), (b) (prohibiting processing operations for which the data protection authority has rendered a negative opinion) and (c) (providing for an administrative sanction in case of failure to consult the data protection authority) of that paragraph.

3) **A certification mechanism for transfers to third countries**, enabling controllers or processors who are not established in the EU to demonstrate compliance with European requirements and receive data transfers from the EU, **should be introduced**.

● We support the Presidency's proposal to explore the use of such a mechanism (see paragraph 16 of the working document). In particular, such a mechanism could enable controllers and processors established outside the EU to demonstrate compliance with European data protection legislation.

● At this point, we have reservations about a mechanism allowing data transfers on the basis of codes of conduct (see paragraphs 15 and 16 of the working document and Article 38). By definition, those would have been adopted by the recipient in the third country and, consequently, compliance with them would not be monitored by European data protection authorities.

● We would point out that a certification mechanism would better guarantee compliance with European requirements and make it possible to carry out checks on compliance as well as to provide means of redress to the persons concerned enabling them to enforce their rights with regard to personal data. **In this connection, please refer to our note presenting the new mechanism that we would like to see introduced (11715/14, dated 9 July 2014)**. We will submit drafting suggestions in relation to that mechanism as soon as possible

CROATIA

Attention is drawn to the HR comments already listed in the footnotes 29, 31, 33 and 35.

- The question in point 9. – We believe that it is sufficient to define high-risk situations, and further clarify the derogation of the same.
- The question in point 10. – We has already made comment on this as referred to in footnote 31.
- The question in point 12. – We are stand that by the existing provisions sufficient levels of protection is achieved, which is based on the principle of risk based approach.
- The question in point 14. – We believe that the offered options b) and c) are appropriate instruments of legal certainty in cases of prior consultation.
- As regard Article 32, Para. 3. we suggest to add the following wording:

c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an **equal and effective** manner; or

d. it would adversely affect a substantial public interest **which is recognized by the law.**

HUNGARY

Presidency proposal regarding the risk-based approach

1. In general, Hungary is in favour of the concept of risk-based approach underlying the draft Regulation. According to our interpretation, this concept means that the risks – presented by the data processing – are assessed by the controller according to the aspects reflected in recital (60). However, on the one hand the "high risks" presented by the processing are specified in Article 33 para. 2., on the other hand the circle of those risks can be broadened by the national supervisory authorities according to Article 33 para. 2a. and 2b.

2. Concerning recital (60), Hungary deems it necessary to broaden the exemplificative enumeration of risks presented by data processing which trigger appropriate measures to be carried out by the controller with the aspects of the source of data (data subject or third person) and the manner of processing (automatic or manual).
Therefore Hungary suggests the following amendments to recital (60):

> 60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation, such as keeping a record, implementing technical and organisational measures for ensuring an appropriate level of security or performing a data protection impact assessment. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:
>
> - where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage; or
> - where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;

- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects**;**
- **where the data have not been obtained from the data subject;**
- **where personal data are processed by automated means.**

3. On the one side Hungary deems the definition of low risk in the draft Regulation only necessary if it triggers legal consequences, on the other side we consider the attempt rather dubious to be able to give a proper definition seeing that low risk can be characterised with the lack of high risk triggering factors.

4. In our opinion the current level of legal protection would be subdued, therefore we cannot support that the supervisory authority is only able to give an opinion on the planned data processing operation but cannot prohibit it if it is against the law (Article 34). Hungary deems it necessary to enable the DPA to prohibit the planned data processing operation if it seems to be obviously against the law and there should be only a very narrow set of exceptions to this rule (e.g. data processing established in Union or Member State law).
Hungary therefore suggests the following amendment to Article 34:

3a. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 is against the Regulation and endangers the rights and freedoms of data subjects – except when the basis for processing is provided for in Union or Member State law – it shall prohibit the intended processing.

5. Hungary is in favour of broadening the national legislator's room for manoeuvre in respect of the determination of the supervisory authority's competence regarding the controlling of the correct application of the codes of conduct and releasing certifications.

6. In recital (60c) we do not agree with the following amendment: *"which cannot be mitigated by reasonable measures in terms of available technology and costs of implementation"*. We think that it is not supported by the normative text of the Regulation and this amendment restricts the obligation of the data processor to consult with the supervisory authority to a very limited amount of cases. Furthermore, it is obvious that the data controller is unable to assess the possibility of the mitigation of risks and that is why the consultation with the supervisory authority is needed.

7. In recital (67) the meaning of the amendment of *"personal rights and freedoms"* is not clear, consequently, Hungary suggests deleting the expression "personal".

8. The aim and the added value of the last paragraph of recital (74) is not completely clear for us, furthermore, this provision is not reflected in the normative text of the Regulation.

9. Hungary maintains its reservation on Article 22 para. 2a.

10. As previously articulated, we do not agree that according to Article 25 para 2. point (b) only the controller employing more than 250 persons has the obligation of designation of a representative in the Union. We believe that on the one hand there is no connection between the number of employees and the riskiness of the data processing operation, on the other hand this provision would make the obligation completely superfluous. We would like to draw attention to the fact that the designation of a representative is important not only in cases of risky data processing operations but in any case, since it facilitates data subjects to exercise their rights. We would like to add our comment to the footnotes.

11. We suggest the deletion of Article 28 para. 4. point b) because we do not agree with the distinction linked to the number of the employees, furthermore, in our opinion there is no added value in point b) compared to point c).

12. In Article 33 para. 2. point b) Hungary is in favour of the inclusion of data on children and biometric data, but we do not agree with the following wording: *"and legitimate expectations of the data subject are not met, for example owing to the context of the processing operation"*, because it would narrow down the obligation of carrying out a data protection impact assessment to an unjustifiable narrow circle.

13. In Article 33 para. 2a. and 2b., we generally support the DPA being able to extend the requirement for a data protection impact assessment to further processing operations which present specific risks to the rights and freedoms of the data subject. Nevertheless, we have serious concerns about the implementation of the rules for the following reasons:

- The territorial scope of the list published by the supervisory authority is ambiguous. The unified application of the regulation would be promoted if the same type of data processing operations triggered the requirement for data protection impact assessment in each Member State. This aim is enhanced by the application of the consistency mechanism as well. However, this would amount to the consequence that before starting any data processing the controller needs to check all the lists published by the DPA's in the EU and EEA.
- Is there any legal consequence, if so, what sort of legal consequence will be incurred by the list published by a DPA on the already on-going processing operations? Similarly, if a DPA confirms that a data processing operation poses specific risk and therefore a data protection impact assessment is required, to what extent does it affect the on-going data protection operations in the Member State concerned or in other Member States?

14. The added value and the aim of Article 33. para. 3a. is ambiguous; therefore it should be further clarified and in Hungary's view it should rather be moved to a recital considering the general content of the provision, as it is not exclusively linked to data protection impact assessment.

15. We maintain our opinion regarding Article 34. para. 1. which does not specify properly the cases of the obligation of prior consultation, since the concept of a "high degree of specific risk" is too vague.
Furthermore it is not completely clear whether the abovementioned provision is identical with the expression "high risk" in Article 33. If the meaning of these expressions is identical, we suggest applying consistent terminology.

16. As we articulated before, Hungary is of the opinion that ensuring the competence for the supervisory authority to be able to prohibit the future data processing operations is essential.

17. As far as Article 35 para. 1. is concerned, we still do not agree with the provision. It is not completely clear that for a data processor which operates in more than one state, which Member State's law can order to designate a data protection officer. Furthermore, we think that the obligatory cases should be included in the Regulation which could be broadened by the sectorial legislation.

THE NETHERLANDS

1. Under the Cypriot and the Irish Presidencies extensive discussions were held on Chapter IV of the Regulation. Although much important progress was made during the preceding Presidencies, the Dutch delegation expressed serious concerns both in the Dapix Working Party, and at the JHA Council meetings in December 2012 and March 2013 on whether the Regulation addresses data controllers appropriately.

2. In order to assess the effects of the Regulation as proposed by the Commission on the Dutch economy an evaluation was conducted. The outcome of the evaluation[15] was that administrative burdens will lower slightly (from € 1,7 mln/year to € 1,5 mln/year), but compliance costs will rise significantly (from € 70 mln/year to € 1,1 bln/year - € 1,4 bln/year). The evaluation made it clear that the highest costs are a consequence of the documentation requirement (article 28), the data protection impact assessment requirement (article 33) and the requirement to designate a data protection officer (article 35).

3. The Dutch Delegation does not deny nor challenge the expected benefits of the Regulation. The Dutch Delegation accepts the fact that in a networked world costs associated with data protection will rise. Yet a fair balance must be struck between the risks for data subjects and the requirements and burdens on data controllers and processors. Should the Regulation fail to do so, compliance will remain insufficient, notwithstanding the considerable enforcement powers of the data protection authorities. The risk based approach is the way to prevent that happening. The Dutch Delegation is therefore in agreement with the Presidency that where the data protection risk is higher, more detailed obligations would be necessary, and, consequently, where the risk is comparably lower, the level of prescriptiveness must be reduced.

[15] Evaluation of the EU Data Protection Regulation, Sira Consulting, Nieuwegein, 31 May 2013. Available on request to the Dutch Delegation.

4. It is therefore important to address or define the high risk for data subjects, which justifies more detailed requirements of data controllers. Procedural requirements to address the risk, as introduced by the Irish Presidency in Article 22, are an important safeguard. However, the use of substantive criteria to define or limit the risk, not just in the recitals, but also in the Articles, will offer more clarity and legal certainty as to the extent of the requirements of data controllers and processors. Substantive criteria on risks have already been adopted in Recital 60. The Dutch Delegation is keen on adopting the most important of these criteria - which refer to the values data protection aims to protect - in the Articles 28, 31, 32, 33 and 34 in a coherent way.

5. During the Hellenic Presidency discussions on aspects of the risk based approach were resumed. On the basis of the achievements under the Hellenic Presidency the Dutch Delegation has worked on proposals on the Articles 33 and 34. The core of these proposals is that data protection impact assessments should only be mandatory if the processing is likely to present a high risk for the rights and freedoms of data subjects, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or ay other siginificant economic or social disadvantage. The likelihood must be assessed by the controller on the basis of a "reasonableness test" which is in the domain of his responsibility, pursuant to Article 22. If the outcome of the data protection impact assessment is that the existence of a high risk cannot be mitigated by reasonable measures in terms of available technology and costs, according to the controller, the controller can request an authorisation by the data protection authority. The data protection authority should have the power to grant the authorisation under conditions in order to mitigate the risks, or refuse the authorisation altogether, if it finds that the risks are unacceptable. Decisions of the data protection authority are subject to judicial scrutiny, pursuant to Article 74. Authorisations offer legal certainty, whereas this remains uncertain when only a consultation of the data protection authority is mandatory. Moreover, data protection authorities can draw a clear line between informal talks and the use of formal powers, which is important for their procedural position in subsequent court cases.

6. The substantive risk criteria proposed by the Dutch Delegation can also be used to limit the extensive documentation requirements pursuant to Article 28, and to limit the data breach notification requirements pursuant to Articles 31 and 32. On Article 28 it must be borne in mind that for the protection of data subjects' rights clear and concise information policies pursuant to Articles 14 and 14a of the Regulation appear to be more important than the keeping of extensive records by data controllers. Although data breach notifications are a very important proposal, it is important to prevent an overflow of notifications in order to maintain effectiveness and avoid unnecessary costs.

7. The Dutch Delegation underlines the importance of data protection officers. Data protection officers offer can offer important incentives in data protection awareness raising in both public and private sector organisations. Data protection officers may therefore be entrusted with a general duty to be aware of the risks associated with the processing. The designation of a data protection officer is an investment made by the controller. Incentives to designate data protection officers should therefore be introduced. Since the duties of a data protection officer naturally involve having an oversight of processing operations, its purposes, its context and its associated risks, reducing the administrative burdens of the documentation requirement on controllers who designate a data protection officer should be considered.

8. The text in this document is based on document 11481/14, issued by the Italian Presidency on 3 July 2014. NL text proposals are in **bold and underlined** type.

60c) Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks **related to the processing**, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by (...) codes of conduct, (...) certifications, guidelines of the European Data Protection Board or through the designation of a data protection officer or, where a data protection impact assessment indicates that processing operations involve a high degree of (...) risk(…), **which cannot be mitigated by reasonable measures in terms of available technology and costs of implementation**, through **an authorisation by** the supervisory authority prior to the processing.

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 obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those processing operations which are likely to present (...) **high** risks to the rights and freedoms of data subjects by virtue of their nature, their scope, (...) their purposes (…), or their context. In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the (...) risks, taking into account the nature, scope, (...) purposes **and context** of the processing and the sources of the risks, which should include in particular the envisaged measures, safeguards and mechanisms **for mitigating those risks in order to ensure** (...) the protection of personal data and for demonstrating the compliance with this Regulation. **The likelihood of the presence of the risk should to be assessed by the controller, since the Regulation requires him to implement data protection policies.**

74) Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a high degree of **residual** risk to the rights and freedoms of data subjects, such as excluding individuals from their rights or giving rise to **a disproportional invasion of privacy**, unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of (...) new technologies**, the data controller should apply for an authorisation with the supervisory authority (...)** prior to the start of the processing activities. **The supervisory authority should be competent to issue a permanent, temporary or conditional authorisation, if it finds the risks can not be mitigated by reasonable mesaures in terms of available technology and costs of implementation to be taken by the controller . (...) The supervisory authority should be competent to refuse the authorisation if the risks can not be mitigated or the processing operations would otherwise not be in compliance with the Regulation.** The supervisory authority should respond to **an application** (...) within a defined period (…). (...).

74a) A (...) consultation should (...) take place in the course of the preparation of a legislative or regulatory measure which provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing.

Article 28

Records[16] of categories of personal data processing activities [17]

…….

4. The obligations referred to in paragraphs 1 and 2a shall not apply to:

(a) (…)[18]

(aa) controllers who have designated a data protection officer, pursuant to Article 35;

(b) controllers who have a valid certificate, pursuant to Article 39;

(c) an enterprise or a body employing fewer than 250 persons**, unless the processing it carries out involves a high risk for the rights and freedoms of data subjects, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage for the data subjects,** having regard to the nature, scope and purposes of the processing[19]; or

5. (…)

6. (…)

---

16 PL and SK suggested to specify that the records could be kept 'in paper or electronically', but it was decided to keep the wording technologically neutral.

17 AT and SI scrutiny reservation. UK stated that it thought that the administrative burden caused by this Article nullified the benefits if the proposed abolition of the notification obligation. DE, LU, NL and SE shared these concerns.

18 COM reservation on deletion.

19 Many delegations criticised the appropriateness of this criterion: AT, BE, DE, DK, ES, FR, GR, IT, LT, LU, NL, MT, PT, and SE. At the suggestion of BE, the criterion was narrowed in the same way as in Article 25(2)(b).

Article 31

Notification of a personal data breach to the supervisory authority[20]

1. In the case of a personal data breach **which is likely to create a high risk for the rights and freedoms of data subjects, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage** for the data subjects, 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.

…….

[20] AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

Article 32

Communication of a personal data breach to the data subject[21]

1. When the personal data breach is likely to create a high risk for the **rights and freedoms** of the data subject**, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage for the data subjects**[22], the controller shall (…)[23] communicate[24] the personal data breach to the data subject without undue delay.

……

[21] AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded. NL thought there should be an exception for statistical data processing. FR thought that the possible application to public/private archives required further scrutiny.

[22] BE and SK scrutiny reservation. BE suggested adding: 'or creates a risk for the data subjects'.

[23] AT, PT and SE clarified there is no valid reason why the data subject should always be informed after the DPA. Therefore this part has been deleted. DE however proposed to start this paragraph by stating: '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'

[24] PL suggested specifying this could be done either in paper or electronic form.

Article 33

Data protection impact assessment [25]

1. Where the processing, taking into account the nature, scope, purposes or context of the processing, is likely to present **a high** [26] **risk for the rights and freedoms of data subjects, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage for the data subject**[27]**,** the controller **(…)**[28] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[29].

1a. The controller shall seek the advice of the data protection officer, where applicable, when carrying out a data protection impact assessment.

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

[(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[30] are based that produce legal effects concerning data subjects or severely affect data subjects[31];]

---

25 ES, HU and UK scrutiny reservation; FR thought that the possible application to public/private archives required further scrutiny.

26 ES thought that such assessment should not be required in all cases and wanted to restrict the scope of the Article. ES, FR, LU, PT, RO, SK, SI and UK warned against the considerable administrative burdens flowing from the proposed obligation.

27 BE scrutiny reservation.

28 Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deletion.

29 ES had proposed exempting certified processing operations. BE, CZ, EE and had proposed exempting a controller who had appointed a DPO.

30 BE, supported by PL, 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.

31 FR thought profiling measures might need to be covered by this Article, but this type of processing is largely covered by paragraph 2(a). PL wanted to keep the text in brackets.

(b) processing of [special categories of personal data under Article 9(1), data on children, biometric data] or data on criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals **(…)**[32] [and legitimate expectations of the data subject are not met, for example owing to the context of the processing operation];

(c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (…)[33];

~~(d) (…)[34];~~

~~(e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects[, or because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale]~~[35].

---

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

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

~~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.~~ [36]

~~2b. Prior to the adoption of the list the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.~~ [37]

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risks ~~for rights and freedoms of data subjects,~~ **referred to in paragraph 1** the measures envisaged to address the risks[38] including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[39] taking into account the rights and legitimate interests of data subjects and other persons concerned[40].

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment .

---

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

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

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

4. (…)[41]

5. **(…)** [42]Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question**,** paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[43].

6. (…)

7. (…)

[41] BE, FR indicated that this was a completely impractical obligation. NL and COM were in favour of maintaining it.

[42] The reference to "public authority or body" as a controller was deleted because the nature of the entity is not the appropriate criterion, but rather the fact that the controller is authorised/obliged to process the data pursuant to legal obligations under national/EU law. This provision should be read in conjunction with paragraph 7 of Article 34.

[43] IT scrutiny reservation. DK, IT and COM think the wording of this Article could be aligned to the wording of recital 73, as the latter is more broadly drafted than the former.

Article 34

Prior (…) authorisation[44]

1. (…)

2. **The controller (…)[45] shall apply for an authorisation by 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 any of the risk, referred to in Article 33, paragraph 1, and these risks cannot be mitigated by reasonable measures in terms of available technology and costs of implementation to be taken by the controller** [46] [47].

2a. **The supervisory authority is competent to issue a permanent or temporary authorisation. The supervisory authority is competent to issue a conditional authorisation, in order to further mitigate the risks, referred to in Article 33, paragraph 1.**

2b. The supervisory authority is competent to refuse the authorisation if it is of the opnion that:

a. the risks, referred to in paragraph 2, are insufficiently identified, insufficiently mitigated by reasonable measures in terms of available technology and costs of implementation to be taken by the controller, or unacceptable;

---

44 ES, HU and UK scrutiny reservation; DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. See revised recital 74, which clarifies the scope of the obligation.

45 Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deleting processor.

46 FR and SE scrutiny reservation on the concept of a high degree of specific risks. It was pointed out that such assessments might be time-consuming. IT thought there should be scope for consulting the DPA in other cases as well.

47 DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

b. the intended processing would otherwise not comply with this Regulation.

2c. The supervisory authority is competent to revoke an authorisation if the data controller does not comply with the attached conditions.

3. The supervisory authority shall within a maximum period of six weeks following the application for authorisation transmit its decision on the application to the data controller(…)[48]. This period may be extended for a further period of six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay[49].

4. (…)

5. (…)[50]

6. When applying for an authorisation pursuant to paragraph 2, the controller (…) 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 (…).[51].

---

48 Drafting amended in order to take account of the concern expressed by several delegations that a sanctioning power for DPAs would be difficult to reconcile with (1) the duty on controllers to make prior consultation under the previous paragraph (DE, DK, NL, SE, SI) and (2) the freedom of expression (NL, PL, SI).

49 ES, NL and SI scrutiny reservation. FR thought that for private controllers an absence of consultation or a negative DPA opinion should result in a prohibition of the processing operation concerned, whereas for public controllers, the DPA could publish a negative opinion, but should not be able to stop the processing.

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

51 DE thought this paragraph should be deleted.

7. Member States shall consult the supervisory authority during the preparation[52] of proposals for legislative or regulatory measures which provide for the processing of personal data and which may severely[53] affect categories of data subjects by virtue of the nature, scope or purposes of such processing.

7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health[54].

8. (…)

9. (…)

Article 37

Tasks of the data protection officer

1. The data protection officer **shall have** the following tasks:

(a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation (...);

(b) to monitor compliance with this Regulation and with 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;

---

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

53 COM reservation, in particular regarding regulatory measures: this threshold is not present in the 1995 Directive.

54 DK, NL, PL, SE scrutiny reservation.

(c) (...);

(d) (...);

(e) (...);

(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

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

(h) to act as contact point for the supervisory on issues related to the processing of personal data, including prior **authorisation** referred to in Article 34 and consult, as appropriate, on any other matter.

2. (...)

2a. The data protection officer shall perform his duties, pursuant to the Regulation with due regard to the risks associated with the processing operations, taking into account the purpose, nature and context of the processing

AUSTRIA

Point 9 of the Presidency document (on Articles 22 and 23)

In Austria's view, it is important that the enacting part should include an illustrative list of criteria indicative of a moderate or high level of risk associated with a data processing operation.
In contrast, it would not seem helpful, as far as the structure of the legislation is concerned, for the enacting terms of the General Data Protection Regulation to feature a definition or a list – even just of examples – of habitually low-risk data processing operations, not least because there are a great many such applications.

However, controllers putting the risk-based approach into practice would benefit from having as up-to-date a list as possible of typical low-risk scenarios available to them. The following solution would be an option: Alongside the more resource-intensive "impact assessment", Article 22 or Article 33 could set down an explicit obligation for the controller to carry out a preliminary risk assessment/rough check/simple test. The rough check would merely have to establish in which category of risk (low or moderate-to-high) a planned processing operation would be likely to fall. If the rough check assessed the risk as low, the more in-depth impact assessment would not be carried out.

The rough check could be made considerably simpler by having a list of processing operations typically presenting a low risk, as described above. As in paragraphs 2a and 2b of Article 33, the task of drawing up and publishing such a list could be given to the supervisory body for data protection or, in matters of cross-border significance, to the European Data Protection Board. Austria has long had such a system, defining so-called "standard applications", which present a low risk and do not require authorisation from the authorities, in an implementing act for the national data protection act.

Crucially, this exemption from authorisation applies only if the intended processing operation does not go beyond the specification for the relevant "standard application". That specification is defined in terms of purposes, categories of data processed, groups of data subjects and recipients, maximum retention period and any security measures. By way of illustration, we refer to the example in Annex 1 (*Standardanwendung A022 "Kundenbetreuung und Marketing für eigene Zwecke"* (Standard application A022: "customer service and marketing for internal purposes")). The added value of these "standard applications" is that they are more than just a list, also providing the controller with general guidance on how to organise the processing appropriately.

Point 10 of the Presidency document (on Article 26)

In Austria's view, the arrangement provided for in Article 26(2) should be maintained. We are against weakening it by adding "where relevant". In practice, service contracts are typically based on templates and standard clauses, which can readily be adapted to the specific situation as required. The burden on companies does not, therefore, seem unduly heavy. To achieve the same standard of protection throughout the EU, it is of great importance that minimum standards for such contractual content should be laid down in the General Data Protection Regulation. The relationship between the service provider and the controller in the case of cloud computing, which is one of effective dependency, undeniably poses a particular problem. It is therefore all the more important that certain obligations from the General Data Protection Regulation should apply directly to service providers too (see, for example, Article 30(1)).
Besides, preventing excessive concentration among cloud service providers, and thus offering sufficient choice to controllers, remains a matter of competition policy.

Point 11 of the Presidency document (on Article 30)

We have no objections to the proposed Article 30(1a).

We would also like to point out that data processing operations carried out in the public interest may sometimes necessitate more stringent security requirements, which would take priority over the issue of cost. It would therefore be worth considering adding a clarification to the effect that Member States are permitted to lay down specific security requirements for the public sector by way of national data protection rules. Such requirements could have an indirect effect on the private sector (for example, definition of the security requirements for granting private healthcare providers (self-employed doctors, physiotherapists, etc.) access to the public health service's electronic files). A possible solution for this in the legislation would be an insertion in the last sentence of the second subparagraph of Article 6(3):

"Within the limits of this Regulation, the controller, processing operations, processing procedures, including measures to ensure lawful, fair ***and secure*** *processing, may be specified in this legal basis."*

Point 12 of the Presidency document (on Article 31)

Austria – like Poland – sees added value in notifying the data protection supervisory authority of data breaches even in cases where there is no obligation to inform data subjects directly.
This would enable the collection of valuable data (including statistics) about data security problems in general, and allow preventive measures to be suggested where appropriate.

Point 13 of the Presidency document (on Article 33)

Article 33(1):

Simplifications could be provided to accommodate certain uses of sensitive data, namely uses that are very frequent and always of the same nature, such as invoicing for medical services. In concrete terms, the obligation to carry out an impact assessment and consult the data protection supervisory authority could also be waived if the purposes, categories of data processed, groups of data subjects and recipients, maximum retention period and any security measures exactly fit specifications laid down either by the national supervisory authority or by the European Data Protection Board in the form of a "standard application". An example of this can be found in Annex 2 (*SA028 – Verrechnung ärztlich verordneter Behandlungen und diagnostischer Leistungen durch freiberuflich tätige Angehörige der medizinisch technischen Dienste, klinischen Psychologen und Psychotherapeuten* (SA028 – Invoicing by clinical psychologists, psychotherapists and certain other groups of self-employed healthcare professionals other than doctors, for treatment and diagnostic services prescribed by a doctor)).

Article 33(2), introductory clause:

We note as a basic principle that the list of criteria in Article 33(2) for data processing operations that present a high risk should certainly not be exhaustive. For that reason, the words "in particular" should be inserted at the beginning of paragraph 2 – as in the original Commission proposal.

Article 33(2), points (b) and (e):

In principle, it makes no difference from the perspective of the person whose fundamental rights are involved whether he or she is the only person affected by a use of data or whether there are a great many other data subjects. For example, even a single camera in a public or semi-public area may be the instrument of a serious infringement of fundamental rights, if it is directed at the private sphere (private home or land) of even one individual. Accordingly, the criterion "large scale" is of little use; we are in favour of efforts to avoid using it as the sole basis for assessing the risk.

Point 14 of the Presidency document (on Article 34)

Austria is able to support all three options, subject to the following:
In the case of option a) we additionally note that if the data protection supervisory authority continues not to respond after deadlines for it to make a decision have passed, processing operations should not be prohibited automatically.
As regards option b), a negative opinion on the part of the data protection supervisory authority should not have the force of a formal, legally enforceable decision. Nor, indeed, does it need to, as a law-abiding controller will, as a rule, respect the opinion given by the data protection supervisory authority in response to his or her request. If that controller failed to do so, the authority should of course be able, in exercising its supervisory powers, to issue a formal prohibition if necessary. The controller would then have the usual right of appeal.

Point 15 of the Presidency document

Article 33(3a):

We have no objections in principle.

Article 38(1a), point (f):

We have no objections, provided that in the context of Article 42(2), the codes of conduct may form a basis for transfer to third countries only if there are given binding legal effect by a contractual agreement and thus also grant rights to data subjects.

Point 16 of the Presidency document (on Articles 38, 38a and 39)

Austria believes that primary responsibility for monitoring codes of conduct should not lie with the data protection supervisory authority. The institutions that produced the codes of conduct should perform that task. Certification of the controller or of processing operations based on appropriate check-lists should, in principle, be carried out by auditors/certification service providers authorised by the State to carry out such work, and not by the data protection supervisory authorities themselves. However, Member States should have the option to authorise data protection supervisory authorities to act as certification service providers too.

POLAND

Poland supports the introduction of the risk-based approach in the draft Regulation from the very beginning. We hope that it will provide benefits in particular to small and medium-sized enterprises.

With respect to **Article 25**, Poland sustains its objections expressed in footnote 22. In our opinion, the criterion of 250 persons should be replaced or supplemented by another criterion, which fits better in the principle of the risk-based approach (for example, a criterion of the number of records processed).

With regard to **article 26 paragraph 2**, in our opinion, it should retain its current shape. Contracting of personal data processing constitutes an act of considerable importance, hence requires adequate legal certainty. In our view, the current wording, which includes standard list of items that should be included in every contract or other legal act binding the processor to the controller, ensures legal certainty.

When dealing with **Article 31** we should try to reduce the risk of flooding DPAs with irrelevant notifications and allow them to focus on these breaches of data protection, which may affect the rights and freedoms of the data subjects. However, at the same time Poland believes that **Article 31 paragraph 1a should be deleted** – the controller shall always, when it is required by law, notify the supervisory authority of a breach, so that the supervisory authority can determine whether the controller took appropriate action. The follow-up from a DPA in case a notification of the data subject is not required under Article 32 paragraph 3 letter a and b, shall not be obligatory.

In our opinion **Article 33** should include an explicit reference to Article 23 in order to underline that the Data Protection Impact Assessment should also include an analysis regarding the proper implementation of privacy by design and privacy by default. In **Article 33 paragraph 1a** we would like to have “may” instead of “shall” and “where designated” instead of “where applicable” in order to clarify this provision:

*1a. The controller **may** ~~shall~~ seek the advice of the data protection officer, where **designated** ~~applicable~~, when carrying a data protection impact assessment.*

With respect to **Article 33 paragraph 2 letter b** the criterion of "legitimate expectations" is very general and unclear, reducing legal certainty, therefore we are hesitant about this change. We support introduction of **paragraph 3a** in this article, as we are in favour of increasing the role of codes of conduct and other self-regulation mechanisms.

With respect to **Article 34** and question asked in point 14 of the Presidency's paper:

- We are against prohibiting processing operations pending the opinion of a DPA – we should always presume that data controller's actions are lawful. It is controller's responsibility to process data in accordance with all applicable legal requirements. In our view, such a prohibition would constitute a significant disadvantage for EU companies, many of which compete on the global market. We should not require from the EU companies to wait for an opinion which might be issued many weeks after the relevant request is submitted. In any case, a data controller will be responsible for any breach of the Regulation that occurred during this period;
- We are in favour of prohibiting processing operations for which the data protection authority has rendered a negative opinion – negative opinion at this stage means a very high probability for a negative decision of a DPA to be issued in the future;
- We are in favour of providing for an administrative sanction in case of failure to consult the data protection authority.

With respect to **Article 39 paragraphs 2a, 3 and 4**, Poland is of the opinion that DPAs should be able to certify controllers and processors on their own, in addition to certification conducted by accredited bodies.

Poland supports changes made in **Article 39a paragraph 4**. Moreover, in our view, we should consider giving DPAs powers to revoke a certificate by itself, if an accredited body does not do so within the time limits set by a DPA.

ROMANIA

Art. 22 - Obligations of the controller

It is necessary to know which are the criteria which ensure the proportionality of the processing activities when the controller decides to draft own procedures, according to art. 22. We are of the opinion that the reference to proportionality in paragraph 2a: "Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller", is too vague and does not practically ensure the conformity with the stipulations of the regulation.

We request further clarification of the term "policies" (art. 22, paragraph 2) in view of the fact art. 22, paragraph 1 also establishes an obligation of the data controller to implement appropriate "measures" which may lead to certain confusion as regards the data controller's administrative burdens.

SLOVAK REPUBLIC

Recital 71

We deem it necessary to express our reservation towards introduction of a provision "where a new technology is used". Term "new technology" is highly relative and lacks any certainty whatsoever. It is therefore necessary to clarify this term with aim to specify its purpose. Considering the current extreme technological progress it is unfortunate to introduce terms like new technology. Considering the current situation in technological development new technologies are introduced on highly frequent basis and by the day of adoption of the Regulation a new technology will be any technology introduced after this day. We therefore cannot quite imagine application of this provision in practice and we propose its deletion or alteration in following manner:

71) This should in particular apply to newly established large scale processing operations, 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, as well as to processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where **in accordance with achieved state of technological knowledge** 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**.**

Article 22

Definition of risks is in our opinion problematic since it is hard to define risk in advance and risk assessment depends on the context of specific conditions of data processing. It is not possible to take into account all risks even now, not to mention future developments of data processing. Therefore we agree with several other delegations, namely IE and KOM that the definition of risk is not achievable due to the fact that it fully depends on the context of data processing.

Article 26 (2)

We do not deem it suitable solution to lower normative state of this provision and we would like to maintain its current form. Strict definition of controller´s obligations while designating the processor does not hinder contractual freedom and is in our opinion necessary despite the fact that it might seem too prescriptive.

Article 26 (2a)

We would still welcome alteration of this provision which consist of emphasizing that the another processor processes data on original processor´s liability and that another processor shall be for the purposes of this Regulation deemed as original processor. We propose amendment of this provision in following way:

2a. Where a processor enlists by way of contract or other legal act another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. **Another processor processes personal data and provides their protection on processor´s liability. Provisions of this Regulation regarding the processor are binding also for another processor. For the purposes of this Regulation another processor is considered the processor.**

We would also welcome the clarification of term "another legal act" since its placement in recital 63a and in Article 26 (2) and 26 (2a) appears to be contradictory. While in recital 63 this term is introduced as "other legal act under Union or Member State law" in Article 26 (2) and 26 (2a) it lacks the second part and consists only of "other legal act" which may lead to uncertain interpretation. In recital 63a this term clearly states that the possibility to designate a processor may be regulated by a legal act under Union or Member State law. Article 26 (2) and 26 (2a) however appears to state that such a possibility is regulated only by "other legal act" between the controller and the processor which causes confusion and we deem it necessary to clarify these provisions.

Article 33 (2) (c)

We still maintain our opinion stated in the footnote No. 89.

Article 34 (2)

The national DPAs should in our opinion have a possibility to consult and to prohibit further processing based on their negative statement. However we do not deem it appropriate to impose upon controllers the obligation not to process data until provision of statement of the DPA since it has a potential to cause controllers a significant financial harm. Current wording of Article 34 (2) imposes prior consultation as an obligation of the controller therefore it is only logical that breach of this obligation should result in imposition of a fine. We therefore support points b) and c) of proposed options in point 14 of the PRES document.

Article 37

We highly appreciate current wording of this article. We would however like a small amendment in following manner:

Article 37

Tasks of the data protection officer

1. **Before commencement of the processing of personal data in the filing system the data protection officer shall be obliged to assess whether any danger of violation of the rights and freedoms of data subjects arises from such processing. The data protection officer shall be obliged to inform the controller in writing without undue delay of any disclosure of violation of the rights and freedoms of data subjects before commencement of the processing or of disclosure of a breach of provisions of this Regulation in the course of the processing of personal data**. The controller or the processor shall entrust the data protection officer (…) with the following tasks:

Article 38a

We deem it more appropriate to entrust solely national DPAs with the monitoring and certification of codes of conduct. We are not however opposed to the possibility to entrust specific bodies with this obligation, which shall than be delegated to monitor and certificate codes of conduct. In entirety we are of the opinion that the national DPAs are those bodies, which have the highest expertise and are competent to monitor and certify codes of conduct. Same applies to Articles 39 and 39a. We are however in favour of maintaining the possibility for each Member State to delegate other bodies with complete or partial competencies connected with monitoring and certification of codes of conduct.