Council of the European Union

Brussels, 2 September 2014
(OR. en)

12267/2/14
REV 2

LIMITE

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

Interinstitutional File:
2012/0011 (COD)

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

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:

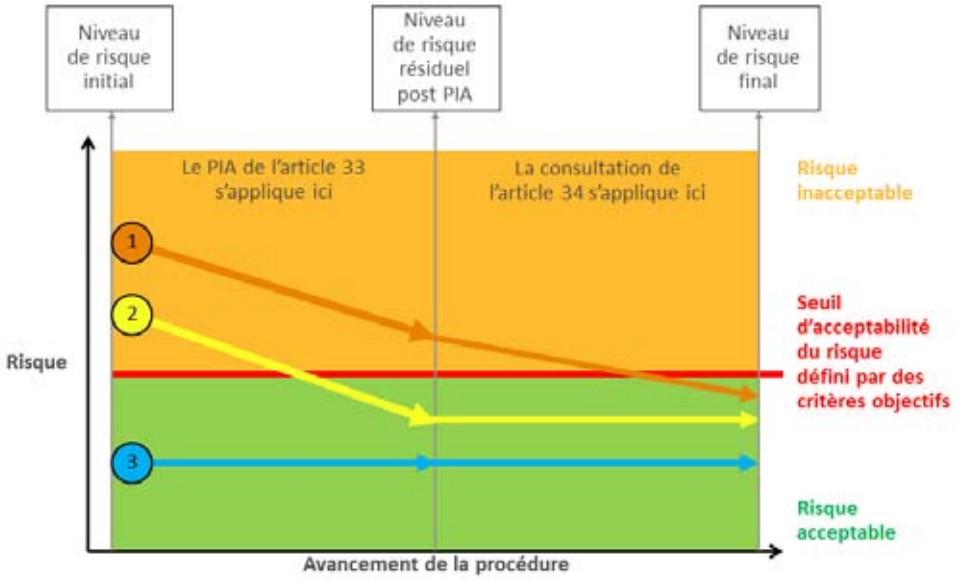
- Point 9, page 3 (art. 22 and recitals 60): BE has a scrutiny reservation on that point. We aren't totally convinced that a definition of low risk could improve the legal certainty. It could be better to talk about acceptable risk or inacceptable risk.

- 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)

GERMANY

Comments and proposals by the German delegation

concerning

Articles 22 - 39a of the General Data Protection Regulation

Germany welcomes the development of risk-based elements in Chapter IV as proposed by the Presidency. Not every kind of data processing poses the same risks to privacy. It is necessary to carry out a multi-level assessment of the risks, especially with regard to measures that create major administrative burdens for the controller and from which the data subject does not benefit.

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 inclusion of risk-based elements is the way to prevent that happening. The German 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, while still protecting the rights of data subjects in a sufficient way.

Based on the risk-based approach the German delegation would like to make the following comments and proposals (changes are made to the Italian Presidency's draft in document 12312/14 and are italic, bold and underlined).

Germany reserves the right to make further comments and proposals to Chapter IV.

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. Risks should be evaluated on an objective assessment, by which its established whether data processing is likely to prejudice 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 ***unlawful or arbitrary*** discrimination, identity theft or fraud, financial loss, ***breach of anonymity or pseudonymity,*** damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage ***for the private life and communications of the data subjects***; or

Comments by the German delegation:

- ***The wording of this bullet point should be identical with the wording in Article 22.***
- ***The German proposal adds one more aspect that is not yet considered enough in the Regulation: "breach of anonymity or pseudonymity".***
- ***To clarify the concerned rights the new wording at the end of the insertion is: "for the private life and communications of the data subjects". With this the German proposal refers to Article 7 of the Charter of Fundamental Rights.***

- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where ***sensitive*** personal data are processed which***, especially if the processing concerns special categories of personal data provided for in Article 9;*** ~~***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;***~~

Comments by the German delegation:

- ***The special categories of data provided for in Article 9 do not have to be repeated in Recital 60. Referring to Article 9 is sufficient.***
- ***Depending on the context processing of other categories of personal data (e.g. the geolocations of a person) might cause high risk situations as well. Therefore, the special categories provided for in Article 9 should be only explanatory.***

  - 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~~.~~***;***

Comments by the German delegation:

The terms "large amount of personal data" and "large number of data subjects" still have to be clarified.

  - ***where the data processing violates - depending on its context and the relationship between controller and data subject - the data subject's reasonable expectations;***

Comments by the German delegation:

The context of data processing and the data subject's reasonable expectations should be a least one of the case groups that may represent high risk situations.

  - ***where the personal data have not been made publicly available to the controller and/or to the public by the data subject.***

Comments by the German delegation:

Especially with regard to social networks and other information society services in some cases it should make a difference if data subjects have been made their personal information publicly available.

60a) (…)

60b) (…)

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 approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer or, where a data protection impact assessment indicates that processing operations involve***s specific*** ~~***a high degree of (…)***~~ risk***s*** which cannot be mitigated by reasonable measures in terms of available technology and costs of implementation. For such ***specific*** ~~***very high degree of***~~ risk***s*** a~~***n authorisation by/***~~consultation of the supervisory authority should take place prior to the processing.

Comments by the German delegation:

- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The German delegation is in favour of "consultation" instead of "authorisation".***

61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes (…) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour in the Union, the controller should designate a representative, unless ~~***the controller is established in a third country ensuring an adequate level of protection, or***~~ the controller is a small or medium sized enterprise unless the processing it carries out involves ~~***a high degree of***~~ ***specific*** risk***s*** for the rights and freedoms of data subjects, having regard to the nature, scope***,*** ***context*** and purposes of the processing or is a public authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.
The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance of the controller.

Comments by the German delegation:

- ***Whether a third country ensures an adequate level of protection should not predetermine the obligation to designate a representative. Still in most cases according to Article 3(2) the General Data Protection Regulation and not the law of the third country will apply so that the need for a representative is not dispensed.***
- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The wording "nature, scope, context or purposes of the processing" should be the same in the whole Regulation.***

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated by means of adherence of the processor to a code of conduct or a certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, 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, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject.

The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.

64) (…)

64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to present ***specific*** ~~***a high degree of***~~ risk***s*** for the rights and freedoms of data subjects, the controller [or the processor] should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (…) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation.

Comments by the German delegation:

The German delegation is in favour of "specific risks" instead of "a high degree of risk".

65) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the (…) risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, 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 risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

67) A personal data breach may, if not addressed in an adequate and timely manner, result in severe physical, material or moral harm to individuals such as loss of control over their personal data or limitation of (…) their rights, discrimination, identity theft or fraud***, breach of anonymity or pseudonymity***, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage ~~***to the individual concerned***~~ ***for the private life and communications of the data subjects***. These cases with ~~***a high degree***~~ ***specific*** risk***s*** are situations, where based on an objective assessment, it is established whether data processing is likely to severely prejudice the rights and freedoms of data subjects. Therefore, as soon as the controller becomes aware that (…). a personal data breach which may result in severe physical, material or moral harm has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose ~~personal~~ 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. 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.

Comments by the German delegation:

- ***The German proposal adds one more aspect that is not yet considered enough in the Regulation: "breach of anonymity or pseudonymity".***
- ***To clarify the concerned rights the new wording at the end of the insertion is: "for the private life and communications of the data subjects". With this the German proposal refers to Article 7 of the Charter of Fundamental Rights.***
- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***

68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it must be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject (…) taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation

68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data (…).

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

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification 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 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 high 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 and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to (…) 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 and which are particularly invasive, for example, on account of their sensitivity, where [in accordance with the achieved state of technological knowledge] a new technology is used on a large scale as well as to other processing operations which present ~~*a high degree of*~~ ***specific*** risks for the rights and freedoms of data subjects, in particular where it is more difficult for data subjects to exercise their rights.

The processing of a considerable amount of personal data, also of sensitive data, should not be considered as being on a large scale, if the processing of these data ***is protected by professional secrecy or other confidentiality obligations*** ~~***and is necessary for but does not constitute the core professional activities of the controller,***~~ such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney.

Comments by the German delegation:

- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***Without the restricting term „is protected by professional secrecy or other confidentiality obligations" theoretically the data could be used by the controller as "by-catch" as long as it would be the controller's secondary business.***

ALTERNATIVE:

This should in particular apply to cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data under Article 9(1), biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is also required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to present high risks for the rights and freedoms of data subjects, in particular 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.

Comments by the German delegation:

The German delegation would like to know why this is seen as an "alternative" to Recital 71. Germany is of the opinion that both "alternatives" could coexist.

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

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

74) 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 very 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 or giving rise to a disproportional invasion of privacy , unlawful or arbitrary discrimination, substantial identity theft, ***severe breach of anonymity or pseudonymity***, 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. Such very high degree of ***specific*** risk***s*** 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. 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 data protection 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.

Comments by the German delegation:

- ***The German delegation is in favour of "very high specific risks" instead of "a very high degree of risks".***

- ***The German proposal adds one more aspect that is not yet considered enough in the Regulation: "severe breach of anonymity or pseudonymity".***

~~ALTERNATIVE:~~

~~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 very high degree of residual 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 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 specific new technologies, the data controller should apply for an authorisation with the supervisory authority (...) prior to the start of the processing activities. Such very high degree of 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. 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 measures 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 (…).~~

Comments by the German delegation:

The German delegation objects to this alternative.

74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

74b) A consultation with the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data that present ~~***a high degree of***~~ ***specific*** risk***s*** to fundamental rights and freedoms of data subjects, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subject.

Comments by the German delegation:

The German delegation is in favour of "specific risks" instead of "a high degree of risk".

75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

76) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risks inherent to the processing for the rights and freedoms of data subjects.

76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

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

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22

Obligations of the controller

1. ~~***Taking into account the nature, context, scope and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of data subjects, t***~~

The controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. ***The appropriateness of the measures and the requirements for the ability to demonstrate compliance depend on the risks the data processing causes for the rights and freedoms of data subjects. Therefore, the controller has to take into account in particular:***

(a) the nature, scope, and purposes of the data processing;

(b) the categories of personal data concerned, especially if the processing concerns special categories of personal data provided for in Article 9;

(c) the origin of the data, especially if they are publicly available or have been made publicly available to the controller and/or to the public by the data subject;

(d) the likelihood and severity of risk for the rights and freedoms of the data subject;

(e) the context of the data processing, especially the relationship between controller and data subject and the data subject's reasonable expectations based on this relationship.

Comments by the German delegation:

Substantive criteria to define high or specific risks are needed. Such criteria are already described in Recital 60. The German delegation is convinced that these definitions should not only be in recitals, but also in Articles. This will offer more clarity and legal certainty as to the extent of the requirements of data controllers and processors.

2. (…)

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.

2b. Compliance with the obligations of the controller may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39 (….).

3. (…)

4. (…)

Article 23

Data protection by design and by default

1. ***When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, the controller shall, with due*** ~~***Having***~~ regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope***, context*** and purpose of the processing, ~~***the controller shall (…),***~~ implement (…) technical and organisational measures appropriate to the processing activity being carried on and its objectives, ***such as***

a) minimising the processing of personal data,

b) anonymising and/or pseudonymising personal data as soon as possible,

c) transparency with regard to the functions and processing of personal data,

d) enabling the data subject to monitor the data processing,

e) enabling the controller to create and improve security features,

f) the purpose limitation principle (including separately collecting and processing personal data for different purposes),

~~***including pseudonymisation of personal data,***~~ in such a way that the processing will meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, ***the extent of their processing,*** the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

Comments of the German delegation:

Scrutiny reservation on the question which level of data protection and security (e.g. the highest available level) should be chosen.

2a. The controller may demonstrate compliance with the requirements set out in paragraphs 1 and 2 by means of a certification mechanism pursuant to Article 39.

3. ***Regardless of a responsibility under data protection law pursuant to Article 4 (5), producers of the products, services and applications referred to in paragraph 1 shall be required to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, and to make sure that controllers and processors are able to fulfil the obligations referred to in paragraph 1 and 2.***

4. (…)

Comments by the German delegation:

- ***The German delegation welcomes the inclusion of a rule on data protection by design and by default. The German delegation is fully aware of the need to be technologically neutral as well as of the administrative fines to be imposed in accordance with Article 79(6)(e). However, the German delegation would be in favour of more specific requirements and objectives with regard to data protection by design and by default to be included in paragraphs 1 and 2.***
- ***Concerning paragraph 1: The wording "nature, scope, context or purposes of the processing" should be the same in the whole Regulation.***
- ***Concerning paragraph 3: The German delegation proposes to require manufacturers and developers to take into account the right to protection when developing and designing products. It is necessary to address producers and developers as the ability of controllers and processors to fulfill their responsibility according to paragraph 1 and 2 depends highly on the technical possibilities to do so. Furthermore, it should be noted that obligations of designers and producers might influence global technical standards and, by that, might improve level of data protection worldwide.***
- ***The rule still needs to be set out in clearer terms where Article 23 makes requirements of the controller which go beyond the principles set out in Article 5 and the conditions for the lawfulness of data processing set out in Article 6.***

Article 24

Joint controllers

1. ***Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers.***

2. Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. The arrangement should designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.

4.~~2~~. ~~Irrespective of the terms of the arrangement referred to in paragraph 1, t~~

The data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers

a) if there is no arrangement between the joint controllers, or

b) if the arrangement has not designated a single point of contact for data subjects within the European Union, or

c) if the arrangement is unclear as to the liability or responsibility of the respective controllers, or

d) ~~unless~~ if the data subject has ***not*** been informed in a transparent manner which of the joint controllers is responsible***, or~~***

e) if the arrangement is unfairly detrimental to the rights and interests of the data subject.

Comments by the German delegation:

- ***Like other Member States the German delegation feels that the rule was not yet sufficiently clear.***
- ***The proposed paragraph 3 sentence 1 derives from the EP proposal.***
- ***Furthermore safeguards are proposed in paragraph 4 to prevent responsibility from being abdicated to the detriment of the data subject, for example to controllers in third countries. The proposed paragraph 4(c) derives from the EP proposal.***

- ***The relationship between Article 24 and Article 26 still has to be clarified (with special regard to cloud computing).***

Article 25

Representatives of controllers not established in the Union

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union.

2. This obligation shall not apply to:

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

Comments by the German delegation:

Paragraph (2)(a) should be deleted. Whether a third country ensures an adequate level of protection should not predetermine the obligation to designate a representative. Still in most cases according to Article 3(2) the General Data Protection Regulation and not the law of the third country will apply so that the need for a representative is not dispensed. Further, the Commission's decisions on adequacy do not guarantee the same level of enforcement of the rights of data subjects and supervisory authority measures as law enforcement within the EU.

(b) an enterprise employing fewer than 250 persons unless the processing it carries out presents ***~~a high degree of~~ specific*** risk***s*** for the rights and freedoms of data subjects, having regard to the nature, context, scope and purposes of the processing; or

Comments by the German delegation:

The German delegation is in favour of "specific risks" instead of "a high degree of risk".

(c) a public authority or body.

(d) (…)

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

3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.

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

Comments by the German delegation:

- ***Recital 63 states that the designated representative should be subjected to enforcement actions in case of non-compliance of the controller. The German delegation is of the opinion that this clause should be not only in the Recital but also in the Regulation.***
- ***Article 28(1) obligates the representative to maintain a record of all categories of personal data processing activities under its responsibility. Article 28(3) obligates the representative to - on request - make the record available to the supervisory authority. Article 53(1)(a) obligates the representative to provide the supervisory authority any information it requires for the performance of its duties.***

Article 78(2) of the original COM proposal stated that "any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller." This clause has been deleted from the draft. Thus, it is not clear which obligations could be enforced against the representative. It should be made clear that supervisory authority or judicial measures and sanctions can be effectively imposed, served and enforced against the representative. Further the question has to be answered how the supervisory authorities enforce their decisions, since on-the-spot-checks in the third country are neither legally possible nor practical.

- ***In accordance with Article 4(14) the representative should also expressly act as a contact person to data subjects, as required in Article 14(1)(a). The relevant addition should be made to Article 4(14).***

- ***Doubts exist whether the criterion in paragraph (2)(b) is suitable. The problems associated with enforcement in third countries are not dependent on the size of the enterprise. Assuming the business compositions mentioned in the EU's impact assessment, that means that 99.8 % of all enterprises in third countries are exempt from the obligation to nominate a representative. In addition, it would be very difficult for supervisory authorities to find out how many people a business employs in a third country. The definition of high or specific risk situations (see Article 22(1) of the German proposal) should be used instead. The European Data Protection Board should be empowered to issue guidelines defining high risk situations.***

- ***Paragraph 3 leaves it entirely up to businesses offering EU-wide internet services where they appoint a representative within the EU. According to the German one-stop-shop proposal (doc. 6637/14 dated 18 February 2014) the lead supervisory authority which is solely responsible for all issues related to a positive EU-wide compliance decision as described in Article 34a of the German proposal is the authority where the business has its representative in the EU. Any data protection supervisory authority is allowed to initiate a procedure to establish non-compliance of data processing (Article 57 of the German one-stop-shop proposal) against the representative within the EU.***

Article 26

Processor[1]

1. ***Where personal data are processed on behalf of the controller, the controller shall be responsible for ensuring compliance with data protection rules. The controller may use a processor only if he determines the purposes and means of the processing of personal data.***

1a. The rights of the data subject and the right to compensation for damages must be asserted against the controller.

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

2. The carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law 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, ***the rights of surveillance*** and stipulating ***the powers of the controller*** in particular that the processor shall:

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

(b) (…)

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

[1] ***DE: scrutiny reservation, especially with regard to the need to study the general question of responsibility for processing (and in particular the way it is to be applied by the phenomenon of cloud computing) in a horizontal way and with regard to the relationship between Article 24 and Article 26.***

(d) respect the conditions for enlisting another processor, such as a requirement of specific prior permission of the controller;

(e) as far as ~~***possible***~~ ***stipulated***, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;

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

(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject**;**

(h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article ***and tolerate and contribute to audits conducted by the controller***.

The processor must immediately inform the controller if, in his opinion, an instruction breaches data protection rules.

2a. Where a processor enlists by way of a contract or other legal act under Union or Member State law 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. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

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

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

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

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

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.

4. (…)

5. (…)

Article 27

Processing under the authority of the controller and processor

(…)

Article 28

Records of categories of personal data processing activities

1. Each controller and, if any, the controller's representative, shall maintain a record of all categories of personal data processing activities under its responsibility. This record shall contain the following information:

(a) the name and contact details of the controller and any joint controller, controller's representative and data protection officer, if any;

(b) (…)

(c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f);

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

(e) the (…) categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries;

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(g) where possible, the envisaged time limits for erasure of the different categories of data~~.~~***;***

(h) ***a general description which allows the technical and organisational measures referred to in Article 30(1) to be evaluated.***

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

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

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

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

(d) where applicable, the categories of transfers of personal data to a third country or an international organisation .

3a. The records referred to in paragraphs 1 and 2a shall be in writing**,** including in an electronic or other non-legible form which is capable of being converted into a legible form.

3. On request, the controller and the processor and, if any, the controller's representative, shall make the record available to the supervisory authority.

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

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

Comments by the German delegation:

- ***This proposal is taken from the original COM proposal.***
- ***Further work on the household exemption has to be done. However, to what extent data protection rules should apply to private persons, the German delegation thinks that in these cases the obligations for private persons as controllers should be strictly limited.***

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

~~***(b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high degree of risk for the rights and freedoms of data subjects, such as 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, context, scope and purposes of the processing;***~~ or

(c) categories of processing activities which by virtue of the nature, context, scope or purposes of the processing are unlikely to result in ***~~a high degree of~~ specific*** risk***s*** for the rights and freedoms of data subjects, ***such as excluding individuals from their rights, giving rise to unlawful or arbitrary discrimination, identity theft or fraud, breach of anonymity or pseudonymity, financial loss, , damage of reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the private life and communications of the data subjects.***

5. (…)

6. (…)

Comments of the German delegation:

- ***The controller's information and documentation requirements were originally tailored to individual data files and classic logging procedures. Due to the problematic nature of log data in terms of data protection law, in automated searches only every tenth query had been used to be logged and comprehensive monitoring had been intentionally avoided.***
- ***The Regulation however contains a direct and total obligation for all controllers. The content and the idea of a documentation laid down in Article 28 is taken from the notification system in Article 19 of the Directive 95/46, which was often seen as a bureaucratic burden for controllers without real benefits for data subjects and DPAs. In a networked world in which data may in some cases be publicly accessible or sent to multiple recipients at the same time they are collected a documentation based on the idea of notifications may not be sufficient for control purposes on the one hand and still raise a lot of administrative burdens on the other hand. However, complete logging of all processing operations, which was foreseen in the original COM draft, would require an almost unimaginable amount of metadata and therefore raises new problems of protecting these protocol data.***
- ***Against this background DE underlines the importance of clear and concise information policies pursuant to Articles 14 and 14a of the Regulation.***

- ***DE also supports those delegations, who want to strengthen the risk-based approach. Deciding whether a data processing procedure or business model takes the rights of data subjects, users or consumers sufficiently into account does mostly not depend on being able to trace every single step in processing the data. 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. DE recommends adopting the most important of these criteria - which refer to the values data protection aims to protect - in the Articles 22, 28, 31, 32, 33 and 34 in a coherent way.***
- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***

Article 29

Co-operation with the supervisory authority

(…)

SECTION 2

DATA SECURITY

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context**,** scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, including ***anonymisation and*** pseudonymisation of personal data, to ensure a level of security appropriate to these risks.

1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, which could lead to physical, material or moral harm, in particular from ***breach of confidentiality***, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. ***With regard to processing carried out in the public interest or in the exercise of official authority vested in the controller, Member State law to which the data controller or processor is subject may specify the measures referred to in paragraph 1 or provide for a higher level of security.***

2a. The controller and processor may demonstrate compliance with the requirements set out in paragraph 1 by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39.

2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3. (…)

4. (…)

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 ***~~a high degree of~~ specific*** risk***s*** for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud***,*** ***breach of anonymity or pseudonymity***, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage ***for the private life and communications of 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.

Comments by the German delegation:

- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The German proposal adds one more aspect that is not yet considered enough in the Regulation: "breach of anonymity or pseudonymity".***
- ***To clarify the concerned rights the new wording at the end of the insertion is: "for the private life and communications of the data subjects". With this the German proposal refers to Article 7 of the Charter of Fundamental Rights.***

~~1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b)~~.

Comments by the German delegation:

In these cases the supervisory authorities should more than ever check if measures required under Article 32(3)(a) and (b) were sufficient.

2. (…) The processor shall ***~~alert and inform~~ notify*** the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 ***and 2*** must at least:

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

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

   (c) (…)

(d) describe the likely consequences of the personal data breach identified by the controller;

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

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.

4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, ***taking into account their severity, by means of appropriately*** comprising the facts surrounding the breach, its effects and the remedial action taken.This documentation must enable the supervisory authority to verify compliance with this Article. (…).

5. ***Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach.***

6. (….).

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to present ***~~a high degree of~~ specific*** risk***s*** for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud***, breach of anonymity or pseudonymity***, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage ***for the private life and communications of the data subjects, or*** severely affect the rights and freedoms of the data subject, the controller shall ***immediately*** communicate the personal data breach to the data subject ***or to the public as soon as appropriate measures have been taken to render the data secure or where such measures were not taken without undue delay and as there is no longer a risk for criminal prosecution.***

Comments by the German delegation:

- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The German proposal adds one more aspect that is not yet considered enough in the Regulation: "breach of anonymity or pseudonymity".***
- ***To clarify the concerned rights the new wording at the end of the insertion is: "for the private life and communications of the data subjects". With this the German proposal refers to Article 7 of the Charter of Fundamental Rights***

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

3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if**:**

a. the controller (…) has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach ***at the time of the data breach***, in particular those that *have the purpose to* render the data unintelligible to any person who is not authorised to access it, such as ***state of the art*** encryption***, anonymisation or pseudonymisation***; or

b. the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or

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 equally effective manner; or

d. it would adversely affect a substantial public interest.

4. (…)

5. (…)

6. (…)

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment

1. Where the processing, taking into account the nature, scope***, context*** or purposes of the processing, is likely to present ***~~a high~~ degree of specific*** risk***s*** for the rights and freedoms of data subjects, such as ***excluding individuals from their rights, giving rise to unlawful or arbitrary*** discrimination, identity theft or fraud***, breach of anonymity or pseudonymity***, financial loss, ***analyses allowing comprehensive conclusions or evaluations about substantial aspects of the personality or behaviour of a data subject,*** damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage ***for the private life and communications of the data subjects***, the controller (…) shall, ***for his or her area of responsibility and*** prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…).

Comments by the German delegation:

- ***The wording "nature, scope, context or purposes of the processing" should be the same in the whole Regulation.***
- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The German proposal adds three more aspects:***
  - ***breach of anonymity or pseudonymity***
  - ***excluding individuals from their rights***
  - ***analyses allowing comprehensive conclusions or evaluations about substantial aspects of the personality or behaviour of a data subject***
- ***To clarify the concerned rights the new wording at the end of the insertion is: "for the private life and communications of the data subjects". With this the German proposal refers to Article 7 of the Charter of Fundamental Rights.***

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

2. The following processing operations ***may*** present ~~***a high degree of***~~ ***specific*** risk***s*** 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];

Comments by the German delegation:

- ***The detailed drafting depends on the discussions on Article 20.***
- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***

(b) processing of ***particularly sensitive personal information, in particular*** special categories of personal data under Article 9(1) (…), ***data on children,*** biometric data or data ~~***on***~~ ***revealing*** criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale;

Comments by the German delegation:

The German delegation shares the concerns of BE, FR, SK and ITA regarding the need for a better definition of "large scale". It should be also clarified what is meant by "decisions regarding specific individuals on a large scale". To ensure legal certainty terms like "decision" and "large scale" need to be defined. Is data processing for the purpose of medical documentation and billing by physicians and hospitals considered to be a "decision regarding specific individuals on a large scale"? How many data sets must be processed in order to qualify for "on a large scale" (1,000, 100,000, 1,000,000 ?). This could be clarified either in article 4 (definitions) or in a recital.

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

(d) 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 reasonable expectations are not met, for example owing to the context of the processing operation;

(e) processing operations involving personal data which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons;

(f) ~~(e)~~ other operations where the competent supervisory authority considers that the processing is likely to result in ***~~high degree of~~ specific*** risks for the rights and freedoms of data subjects, ***~~in particular because they render the exercise by data subjects of their rights under this Regulation more difficult (…).~~***

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)~~ (f)*** of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

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

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risks referred to in paragraph 1***, also in view of Article 30***, the measures envisaged to address the risks including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

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.

4. The controller shall carry out the assessment at the request of the data subjects without prejudice to the protection of commercial or public interests or the security of the processing operations and make it available in an appropriate form.

Comments by the German delegation:

The German delegation is in favour of maintaining this COM proposal.

5. 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.

Comments by the German delegation:

Scrutiny reservation on the question whether there should be the possibility that paragraphs 1 to 3 shall not apply if data are processed in the public interest (e.g. in the interest of public health by hospitals, doctors, laboratories, and so on).

6. (…)
7. (…)

Article 34

Prior (…) consultation

1. (…)

2. The controller ***shall be responsible for carrying out the data protection impact assessment provided for in Article 33 and, where the impact assessment indicates that the processing is likely to present a very high degree of specific risks,*** shall consult the supervisory authority prior to the processing of personal data ~~***where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a very high degree of (…) risk***~~***. The processor shall, on request, assist the controller with respect to the consultation of the supervisory authority.***

Comments by the German proposal:

The German delegation is in favour of "very high degree of specific risks" instead of "very high degree of risk".

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the risks is insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller (…). This period may be extended for a further 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.
4. (…)
5. (…)
6. When consulting the supervisory authority pursuant to paragraph 2, the controller (…) shall provide the supervisory authority**,** with
   (a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
   (b) the purposes and means of the intended processing;
   (c) the measures and safeguards provided to protect the rights and freedoms of data subject pursuant to this Regulation;
   (d) where applicable , the contact details of the data protection officer;

(e) the data protection impact assessment as provided for in Article 33 and

(f) any other information requested by the supervisory authority (…).

ALTERNATIVE:

2. The controller (…) 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 very high degree of 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.

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 opinion that:

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

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 (…). 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.

4. (…)

~~***5. (…)***~~

~~***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.***~~

Comments by the German delegation:

The German delegation is in favour of alternative 1 and objects to alternative 2.

7. 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 that present ~~***a high degree of specific***~~ risk***s*** to fundamental right s and freedoms of data subjects by virtue of the nature, scope***, context*** or purposes of such processing.

Comments by the German delegation:

- ***The German delegation is in favour of "specific risks" instead of "a high degree of risk".***
- ***The wording "nature, scope, context or purposes of the processing" should be the same in the whole Regulation.***

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.

Comments by the German delegation:

Scrutiny reservation. Member State law may differ with regard to prior authorisations. This could lead to restrictions of the free movement of personal data within the European Union.

8. ***The obligations referred to in this Article shall not apply when a data protection officer has been designated. In this case, the data protection officer shall conduct the data protection impact assessment according to Article 33 and, if he has doubts concerning the lawfulness of a data processing, consult with the supervisory authority.***

Comments by the German delegation:

Germany is still in favour of making it mandatory to appoint data protection officers (DPO). Should the Council not agree, the incentives to appoint a DPO should be improved. Germany therefore proposes providing for the appointment of a DPO as an alternative to the prior consultation pursuant to Art. 34, i.e., in those cases in which the data protection impact assessment indicates that data processing is likely to present specific risks. This would also relieve the burden on the supervisory authorities.

9. (…)

Proposal by the German delegation in doc. 6637/14 dated 18 February 2014:

Article 34a
Decision on Compliance

1. Controllers, processors, joint controllers or group of undertakings which have their main establishment in the Union or have designated an representative pursuant to Article 25 (applicants) may on request obtain a Union-wide compliance decision in trans-border cases from the competent supervisory authority, in order to ensure the compliance of data processing with this Regulation.

2. In order to obtain a compliance decision the applicant shall make a request to the supervisory authority. In the request the applicant must describe and explain

(a) the controller, processor, joint controllers or group of undertakings to which the decision shall apply,

(b) the category of data processing practised or planned,

(c) the concrete concept that the data processing is based on and that is to be examined in the compliance procedure,

(d) the legal basis of the data processing pursuant to Article 6 and the measures to protect the data subject pursuant to this Regulation.

(e) the data protection impact assessment as provided for in Article 33 indicating that the processing is likely to present a high degree of specific risks,

(f) a reasonable interest

aa) in a compliance decision, for example in the case of the introduction of new data processing or a processing for which no established practice or, clear opinion of the supervisory authority exists and

bb) in a Union-wide decision, notably the importance of the data processing for a substantial number of data subjects concerned in more than one Member State or the existance of establishments in more than one Member State.

SECTION 4

DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller or the processor may, or where required by Union or Member State law shall, designate a data protection officer.

2. A group of undertakings may appoint a single data protection officer***, if those undertakings act as a single unit for the purposes of contact with the outside world, if they regularly rely on processing within the group of undertakings and if the data subjects are not disadvantaged by the existence of a single data protection officer.***

2a. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

3. The data protection officer shall have the right to take part in regular trainings at the controller's expense.

4. ***The data protection officer shall maintain secrecy about the identity of the data subject and all circumstances which would allow conclusions regarding the data subject unless the data subject has released him from this duty.***

4a. Without prejudice to paragraph 1, the controller or processor may designate a data protection officer in order to comply with the rights and obligations under this regulation.

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

6. ***The data protection officer shall be designated for a period of at least four years. The data protection officer may be reappointed for further terms.***

7. During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.

8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. ***Insofar as the data protection officer, in the course of his or her activities, obtains data in respect of which the management or persons employed by the controller are entitled, on professional grounds, to withhold evidence under the law of the Member State, that right shall also apply to data protection officers and their staff. Whether or not this right is exercised shall be the decision of the person entitled to withhold evidence for professional reasons. Insofar as the right to withhold evidence enjoyed by the data protection officer continues to apply, the relevant documents shall be the subject of a prohibition of confiscation under the law of the Member State.***

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

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

11. ***The Member States may, by law:***

a) stipulate that controllers or processors, are required to designate a data protection officer in cases other than those provided in point (b) of Article 35(1);

b) specify the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

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

2. The controller or the processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations.

3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. ***He or she shall not be penalised by the controller or the processor for performing his tasks.***The data protection officer shall directly report to the highest management level of the controller or the processor.

4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

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 ***and other data protection provisions***;
   (b) to monitor compliance with this Regulation***, with other data protection provisions*** 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; ***monitoring shall also cover personal data subject to professional secrecy or special official secrecy.***

(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 co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;

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

2. (….)

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

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38

Codes of conduct

1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.

1a. ~~***Associations and other bodies representing categories of controllers or processors***~~ ***Controllers, processors or associations thereof*** may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(a) fair and transparent data processing;

(aa) the legitimate interests pursued by controllers in specific contexts ***and the weighing up of interests according to Article 6 (1) (f)***;

(b) the collection of data ***and adherence to purpose***;

(bb) the ***anonymisation and*** pseudonymisation of personal data;

(bc) consent according to Article 7;

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

(d) the exercise of the rights of data subjects;

(e) information and protection of children and the way to collect the parent's and guardian's consent;

(ee) measures and procedures referred to in Articles 22 and 23 ~~***and measures to ensure security (…) of processing referred to in Article 30***~~;

Comments by the German delegation:

Codes of conduct should not apply to IT security measures. The procedure proposed here carries the risk of establishing conflicting standards and procedures for IT security, even if paragraphs 2b, 3 and 4 contain a procedure for the Union-wide application of codes of conduct. Including IT security measures in the catalogue given in paragraph 1a should at least require that the national IT security authorities are included in the procedure to define codes of conduct concerning IT security measures. This is not the case as the procedure is currently formulated.

(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;

(f) the appropriate safeguards applying to transfer of data to third countries or international organisations under the terms referred to in Article 42(2)(d)

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

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

1b. Such a code of conduct shall contain mechanisms ***for monitoring and ensuring compliance with it*** ~~***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 to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2. ~~***Associations and other bodies***~~ ***Controllers, processors and associations thereof*** referred to in paragraph 1a which intend to prepare a code of conduct, or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.

2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.

2b. Where the code of conduct relates to processing activities in several Member States, the supervisory authority shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which may give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.

3. Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, the European Data Protection Board shall submit its opinion to the Commission.

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

5. ~~***The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.***~~ ***The European Data Protection Board shall collect all codes of conduct in a register and shall publish them in the Official Journal of the European Union and in any other appropriate form. The register shall also indicate which data controllers or processors are bound by the codes of conduct.***

Article 38a

Monitoring of codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

2. A body referred to in paragraph 1 may be accredited for this purpose if:

   (a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

   (b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

[2] ***DE: Subject to an exception for codes of conduct for data processing for scientific purposes, which may be anchored in Article 83c or in Article 38 (5) of this Regulation.***

(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;

(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Comments by the German delegation:

In paragraph 5 it should be considered if data protection authorities of other Member States could be given the right, to launch a procedure at the competent supervisory authority with the aim of revoking the accreditation of a body.

Article 39

Certification

1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a. ***The certification procedure should be voluntary and transparent and carried out at regular intervals by expert bodies that have no conflicts of interest, and contribute to the proper application of this Regulation and other data protection provisions, taking account of the specific features of the various sectors and different processing operations.***

2a. The certification shall be issued by the accredited bodies referred to in Article 39a, or where applicable, the competent supervisory authority.

3. The controller or processor which submits its processing to the certification mechanism shall provide the body referred to in Article 39a, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

4. The certification issued to a controller or processor shall be subject to a periodic review by the body referred to in paragraph 1 of Article 39a , or where applicable, the competent supervisory authority,. It shall be withdrawn by the issuing body or authority where the requirements for the certification are not or no longer met.

Article 39a

Certification body and procedure[3]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification and its periodic review may be carried out by a certification body which has an appropriate level of expertise in relation to data protection and is accredited by the supervisory authority which is competent according to Article 51 or 51a.

2. The body referred to in paragraph 1 may be accredited for this purpose if:
   (a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
   (b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;
   (c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;
   (d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The supervisory authorities shall submit the draft criteria for the accreditation of the body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. The body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification [or the withdrawal of such certification] without prejudice to the responsibility of the controller or processor for compliance with this Regulation.

---

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

5. The body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

6. The criteria for certification and the certification details shall be made public by the supervisory authority in an easily accessible form.

6a. ***Without prejudice to the provisions of Chapter VIII, ~~T~~the*** competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

Comments by the German delegation:

It should be considered if data protection authorities of other Member States could be given the right, to launch a procedure at the competent supervisory authority with the aim of revoking the accreditation of a body.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including conditions for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised 'European Data Protection Seal' within the Union and in third countries].

7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7.

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

9. The previous paragraphs shall not affect provisions governing the responsibility of national certification bodies, the accreditation procedures and the specification of criteria for security and data protection. Commission's power to adopt acts pursuant to paragraphs 7 and 8 shall not apply to national and international certification procedures carried out on this basis. Security certificates issued by the responsible bodies or bodies accredited by them in the framework of these procedures shall be mutually recognized.

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*):

78) 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.**[4] 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;

---

[4] 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 **(…)**[5] 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 (…)**[6] **to accidental or unauthorised access, destruction, loss, modification or dissemination of personal data.**

[5] 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.

[6] 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**[7], 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.[8] **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.**[9] 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**[10]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.

---

7 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.

8 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.

9 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.

10 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**[11] 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.

---

11 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.[12] **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.**[13] 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.

---

12 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.

13 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 (...)[14]

[*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 (…)** [15] 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 (…)**[16]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*]

---

14 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.

15 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).

16 *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 (…)**[17]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.

---

[17] 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.

II. Article 33(2)(e) in close connection with articles 33(2a) and (2b) as well as articles 52(1)(fa) and 57(2)(c)

a. Separation of powers, including the power to adopt legislative acts

Firstly, we would like to briefly explain the legal system of Estonia. We understand that it might not be necessary as the misunderstanding of our reservation might have been caused by the translation and/or the shortness of our intervention(s) at the DAPIX meeting. However, to avoid any further misunderstandings, we will shortly describe the separation of powers.

Namely one of the main principle in our constitutional law is the separation of powers (known in EU as the institutional balance) (Estonian constitution § 4). We believe it is not an unknown principle also to other European countries. The powers are divided as follows: legislative (Parliament), executive (Government) and judicial power (Courts).

The legislative power includes the power to adopt legislative acts as well as delegate some of the legislative power to the Government. However, this is restricted by the Constitution, that legislative powers are only attributed to the specific Government institutions such as ministers only based on certain delegation norm adopted by the Parliament (Estonian constitution § 3, § 59, § 86ff). Administrative authorities and government bodies (such as DPAs) are prevented from using the general legislative powers.

Therefore, it will be against our constitution to give the legislative power to the DPA. We believe that this principle does not go against the decisions of the European Court of Justice, whereas the scope of the independence of the DPAs is being explained and stressed. Namely, it points out that "*the guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim.*" Therefore they should be independent and free from external influence regarding their activities (i.e. in particular the supervision and decision-making power), but the independency does not include the legislative drafting power.[18]

To sum up, our constitutional problem originates from the mere fact, that the supervisory authorities do not have the competence (according to our constitution) to adopt legislative acts (i.e. legislative power). However, this might be a general principle in several member states, which means that the difference of opinion might arise actually from the notions "*legislative act*" as well as "*administrative act*" and the content of article 33(2)(e) and (2a).

b. Legislative act vs administrative act

In general, we think that the power given to the DPAs in article 33(2a), in close connection with 33(2)(e), is a legislative power according to our legal system. Following clarifications explain our statement.

Firstly, article 33(2) provides the controller's obligation to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data, where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific/high[19]risks for the rights and freedoms of data subjects. Article 33(2) names the operations, which present specific/high risks, referred to in paragraph 1.

[18] European Court of Justice, Case No. C‑518/07 p 19, p 25 and 30 (and others); (Furthermore: Cases No. C-614/10 and C-288/12).

[19] For the purposes of clarity we have used throughout the text both words "*specific*" and "*high*" as it has been recently changed for article 33(1) and (2) but not for 33(2)(e).

Furthermore, article 33(2)(e) specifically provides that the competent supervisory authority can consider that other operations, than specified in art 33(2)(a) – (d), present specific risks for the rights and freedoms of data subjects. This article on its own does not cause any problems as the DPAs have the right to interpret the law and in certain cases in an administrative proceeding decide that this particular operation is likely to present specific/high risks and the assessment of the impact has to be carried out.

However, article 33(2a) stipulates that 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. Considering the content and the scope of addressees of this list, it is not a mere administrative act of the DPA but a legislative act.

There are three types of legislation: primary legislation (laws of general nature adopted by the Parliament), secondary legislation (ministerial regulations of general nature adopted in accordance with specific delegation norm in the primary law and specifying the primary law) and administrative acts (decisions by the public authorities made while exercising their powers and addressed to an identified number of addressees).

In case of administrative acts, it is possible to distinguish an individual act (an order made to a particular addressee and regulating a particular situation) and general act / general order (an order addressed to persons determined on the basis of general characteristics and regulating an individual case).The differentiation of general orders (possible to issue by the DPA) and legislative acts (possible to adopt only by Parliament or in certain cases by the Government) is an important one and includes several elements. In the current case, we will explain two crucial elements of general orders.

(a) Persons determined on the basis of general characteristics: We do not see the general characteristics, which allow us to determine the persons to whom this decision of the DPA will be addressed/directed. This will apply technically to all controllers, who are planning to engage into processing operations considered to be presenting specific/high risks for the rights and freedoms of data subjects.

(b) Individual case: Individual case is a particular situation, which is identifiable with a specific vital fact or behaviour. We believe that the list will apply to undefined number of cases, not to an individual case.

To sum up, it is not possible to determine the addressees on the basis of general characteristics nor does this list regulate an individual case. Hence, according to Estonian legal system, the list will be considered as an abstract legal provision to regulate undefined number of cases as well as persons. This means that it is a general and abstract regulation, i.e. a legislative act, which cannot be issued by the DPA, who does not have any legislative power and this power cannot be given to them due to the principle of separation of powers.

c. Proposal

Following the previously described reasons and analysis, we have two different alternatives for rephrasing the article 33(2a) and (2b):

1) We would suggest to erase article 33(2a) and (2b) as well as articles 52(1)(fa) and 57(2)(c). This will leave us with the situation that the competent DPAs can still consider other processing operations likely to present specific risks for the rights and freedoms of data subjects. However, this would and should be a case-by-case decision in the administrative proceeding(s). Furthermore, the administrative practice of the DPA can also be considered as an indication to companies, i.e. if in one administrative proceeding the DPA has considered an activity to cause specific risks, then it is highly likely that it will have to make the same decision in a similar case.
   Although, we also believe that article 33(2)(e) might be unnecessary as the same goal would be achieved by adding the words "*in particularly*" or "*for example*" in article 33(2), i.e. leaving the list non-exhaustive and giving the DPAs the possibility to consider other processing operations causing specific/high risks.

2) We would suggest giving the lists named in articles 33(2a) and (2b) an indicative/advisory nature. In this case it would be considered like guidelines or an advisory role/power of the DPA and it would not go against our constitution. Therefore the list will be as an indication to the companies and it is highly likely that the DPA will decide in a specific case with similar processing activities, that it is likely to present specific risks.
Hence our wording proposal for articles 33(2a) and (2b) is following:

*2a. The supervisory authority shall establish and make public a**n advisory** list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.*

*2b. Prior to the adoption of the **advisory** list the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the **advisory** 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.*
Furthermore, for legal clarity, we suggest changing the wording also in articles 52(1)(fa) and 57(2)(c):

*52(1)(fa):establish and make a**n advisory** list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);*

*57(2)(c): aims at adopting a**n advisory** list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2b); or*

III. Article 34 "Prior consultations"

As mentioned in the working party, we would be in favour of exempting the controllers from the obligation of prior consultations, if they have appointed a DPO. We believe that it would be a good balance between the administrative burden of the controllers as well as the rights and freedoms of the data subject. Therefore, we would kindly ask you to add us to the footnote 103 on page 41 of the document No. 11481/14.

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[20] 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.

[20] 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*[21] *of categories of personal data processing activities [22]

…….

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

(a) (…)[23]

(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[24]; or

5. (…)

6. (…)

---

21 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.

22 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.

23 COM reservation on deletion.

24 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[25]

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.

…….

[25] 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[26]

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**[27], the controller shall (…)[28] communicate[29] the personal data breach to the data subject without undue delay.

……

[26] 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.

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

[28] 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'

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

Article 33

Data protection impact assessment [30]

1. Where the processing, taking into account the nature, scope, purposes or context of the processing, is likely to present **a high** [31] **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**[32]**,** the controller **(…)**[33] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[34].

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[35] are based that produce legal effects concerning data subjects or severely affect data subjects[36];]

---

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

31 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.

32 BE scrutiny reservation.

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

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

35 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.

36 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 **(…)**[37] [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 (…)[38];

~~(d) (…)[39];~~

~~(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]~~[40].

---

37 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.

38 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.~~[41]

~~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.~~[42]

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[43] including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[44] taking into account the rights and legitimate interests of data subjects and other persons concerned[45].

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 .

---

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

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

45 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. (…)[46]

5. **(…)** [47]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[48].

6. (…)

7. (…)

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

[47] 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.

[48] 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[49]

1. (…)

2. **The controller (…)[50] 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** [51] [52].

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;

---

49 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.

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

51 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.

52 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(…)[53]. 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[54].

4. (…)

5. (…)[55]

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 (…).[56].

---

53 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).

54 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.

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

56 DE thought this paragraph should be deleted.

7. Member States shall consult the supervisory authority during the preparation[57] of proposals for legislative or regulatory measures which provide for the processing of personal data and which may severely[58] 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[59].

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;

---

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

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

59 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.