



Council of the
European Union

Brussels, 22 September 2014
(OR. en)

12312/2/14
REV 2

LIMITE

DATAPROTECT 109
JAI 630
MI 579
DRS 104
DAPIX 109
FREMP 148
COMIX 403
CODEC 1675

**Interinstitutional File:
2012/0011 (COD)**

NOTE

From: Presidency
To: COREPER

No. prev. doc.: 11481/14 DATAPROTECT 99 JAI 583 MI 513 DRS 91 DAPIX 97 FREMP
136 COMIX 356 CODEC 1556

Subject: Proposal for a regulation of the European Parliament and of the Council on
the protection of individuals with regard to the processing of personal data
and on the free movement of such data (General Data Protection
Regulation)
- Chapter IV

1. Chapter IV has been intensively discussed in DAPIX during the first half of 2013. Whilst at the Council meeting on 6-7 June 2013, all delegations congratulated the Irish Presidency on the very important progress achieved in this regard, a number of issues were still outstanding, in particular the need to further reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach.

2. Following the discussions at DAPIX on 10-11 July 2014 on the risk-based approach, delegations sent in many written comments¹. A revised text was discussed at the DAPIX meeting of 11-12 September 2014 and again at the JHA Counsellors meetings of 19 and 22 September 2014. The Presidency revision following these meetings is attached to this note. **The use of bold text indicates the latest changes.**

3. The Presidency will be inviting the Council to 'close' the text of Chapter IV at the October JHA meeting and therefore is inviting delegations to discuss Chapter IV in its entirety. The main outstanding issues are further explained out hereafter.

General concept of risk:

4. The Presidency has endeavoured to further detail the risk concept referred to in Article 22 and recitals 60. As it would be difficult to arrive at a definition that would stand the test of time, the Presidency prefers to keep the details of this general risk concept in recitals 60 and 60a, rather than putting it into the body of the text. As indicated in the 'horizontal clause' of Article 22 (and other articles of Chapter IV), the risk refers to risk to rights and freedoms of individuals. Recital 60a gives a list of examples of situations that might prejudice the rights and freedoms of data subject.

High risk

5. Recital 60b describes the concept of high risk. In two cases the Regulation imposes duties on the controller which are triggered by an increased level of risk - now referred to as "high risk" - , namely to notify a data breach (Articles 31 and 32) and to conduct impact assessment (Article 33). In two other cases the presence of an increased level of risk previously served as an exception to the so-called SME exemption: SMEs were nevertheless obliged to comply with the obligations (appointing a representative (Article 26) and maintaining records (Article 28)) of which they are generally exempted. As delegations have criticised this SME exemption, the Presidency suggests to delete these exemptions. In case of the duty to appoint a representative (Article 26), the Presidency suggests to use high risk as a criterion for triggering this obligation. Regarding the duty to maintain records, the absence of a high risk may be used as a criterion. However, some delegations are of the opinion that an approach under which the obligations to appoint a representative and maintain records would be triggered only by a high risk as exceedingly narrow.

¹ 12267/2/14 REV 2 DATAPROTECT 107 JAI 625 MI 574 DRS 102 DAPIX 107
FREMP 146 COMIX 395 CODEC 1671.

Consultation or authorisation

6. In the case of consultation (Article 34), most delegations appeared to be of the opinion that the level of risk which triggers it is the same, namely a high risk. However, the consultation of the data protection authority is required only when the data protection impact assessment indicates that processing, in the absence of mitigating measures, would result in a high risk; a mere likelihood does not suffice.

7. The text of Article 34 obliges the controller in certain cases to consult the data protection authority and Article 79(3), letter (i) provides for an administrative sanction in case of failure to consult the data protection authority. Some delegations have suggested to make the consultation optional, but the majority is supporting a mandatory consultation. NL has proposed to turn the consultation procedure into an optional authorisation procedure. In the view of the Dutch delegation, authorisations offer legal certainty, whereas this remains uncertain when only a consultation of the data protection authority is mandatory. Contrary to what is the case for a consultation of the DPA, the DPA decision in case of an authorisation procedure would obviously be binding. This proposal received little support.

Accreditation by national accreditation bodies

8. Certification is one of the mechanisms provided for in the draft regulation in order to allow companies to comply in an easier way with their obligations. At the suggestion of the ES delegation, not only specifically accredited bodies will be able to issue these certifications, but also the National Accreditation Body named in accordance with Regulation (EC) 765/2008.

9. *In the light of above and in view of 'closing' the text of Chapter IV at October Council meeting, delegations are invited to:*
 - ✓ *confirm the Presidency's understanding of the two levels of risk as set out above;*
 - ✓ *confirm that the SME-criterion in Articles 25 and 28 can be deleted and replaced by a reference to the absence of high risk;*
 - ✓ *confirm the Presidency's understanding of the mandatory consultation procedure;*
 - ✓ *confirm that accreditation of certification bodies can also take place by national accreditation bodies*
 - ✓ *lift all reservations on 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 risk for the rights and freedoms of individuals.

60a) Such risks, of varying likelihood and severity, may result from 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 to the reputation, loss of confidentiality, [breach of (...) pseudonymity]², 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 subjects³; (...).

² The reference to the use of pseudonymous data in Chapter IV will in the future need to be debated in the context of a further debate on pseudonymising personal data.

³ HU proposed to add two additional indents: '- where the data have not been obtained from the data subject;' and '- where personal data are processed by automated means'. DE wanted to mention sensitive data, reasonable expectations and whether the data had been made public by the data subject. NL disagreed with DE on sensitive data.

- 60b) The likelihood and **severity** of the **risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a **high risk**. A **high risk** is a risk that involves a **concrete possibility** of prejudice to the rights and freedoms of **individuals** (...).**
- 60c) Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, 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. The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result into a **high risk** for the rights and freedoms of **individuals** and indicate what measures may be sufficient in such cases to address such risk. (...)
- 61) The protection of the rights and freedoms of **individuals** 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. Such measures could consist **inter alia** of minimising the processing of personal data, (...) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. **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, producers of the products, services and applications should be encouraged** 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, to make sure that controllers and processors are able to fulfil their data protection obligations.

- 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, and *the processing it carries out is likely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing as well as the concrete possibility and severity of the risk for the rights and freedoms of data subjects*, the controller should designate a representative, unless (...) the controller 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.

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 also by means of adherence of the processor to an approved code of conduct or an approved 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 purposes 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 risk 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) (...)

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 risk. 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 risk and the nature of the personal data to be protected. (...). In assessing data security risk, consideration should be given to the given risk 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.
- 66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a **high** risk for the rights and freedoms of **individuals**, 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, **concrete possibility** and severity of this risk. 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. Where a data protection impact assessment indicates that processing operations involve a **high** risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

- 67) A personal data breach may, if not addressed in an adequate and timely manner, result in (...) physical, material or moral damage to individuals such as loss of control over their personal data or limitation of (...) their rights, discrimination, identity theft or fraud, financial loss, [breach of (...) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. (...). Therefore, as soon as the controller becomes aware that (...) a personal data breach which may result in (...) physical, material or moral damage 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 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 damage would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.
- 68) (...) 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 (...). **The fact that the notification was made without undue delay should be established** 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 result in a high risk to the rights and freedoms of **individuals** 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 concrete possibility and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk, which should include in particular the envisaged measures, safeguards and mechanisms for mitigating that risk 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 likely to result in a high risk, 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 result in a high (...) risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in 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, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally 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 result in a high risk 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. *The processing of (...) personal data irrespective of the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by professional secrecy (...), such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.*
- 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 **would, despite the envisaged safeguards, security measures and mechanisms to mitigate the risk, result in a high** risk to the rights and freedoms of **individuals** (...), and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted, prior to the start of the processing activities. Such high (...) risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of (...) damage or (...) interference with the rights and freedoms of the data subject. 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, including the power to prohibit processing operations. 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 **the** risk for the rights and freedoms of **individuals**.
- 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 (...), in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

- 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 risk likely to result from the processing for the rights and freedoms of individuals.
- 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 PROCESSOR⁴

SECTION 1
GENERAL OBLIGATIONS

Article 22

Obligations of the controller⁵

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 **individuals**, the controller shall (...) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation⁶.
2. (...)
- 2a. Where proportionate in relation to the processing activities⁷, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

⁴ DK, SI and UK scrutiny reservation on the entire chapter. BE, DE, DK, NL, PT and UK were not convinced by the figures provided by COM according to which the reduction of administrative burdens doing away with the general notification obligation on controllers, outbalanced any additional administrative burdens and compliance costs flowing from the proposed Regulation.

⁵ UK thought this Article could be deleted as it overlaps with existing obligations and it focuses too much on procedures. DE, supported by EE, thought criteria from recital 60 should be set out in the Article; AT that wanted simple criteria in the article so that it would be easy to use in practice.

⁶ UK referred to the danger in maintaining such a vaguely worded obligation, applicable to all controllers, non-compliance of which is liable to sanctions. The Presidency suggests this be taken into account when dealing with sanctions.

⁷ HU, RO and PL thought this wording allowed too much leeway to controllers. AT thought that in particular for the respects to time limits and the reference to the proportionality was problematic.

2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.

3. (...)

4. (...)

Article 23

Data protection by design and by default⁸

1. (...) Having regard to available technology and the cost of implementation and taking account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing the controllers shall implement (...) technical and organisational measures appropriate to the processing activity being carried out and its objectives[, including (...) pseudonymisation⁹], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (...) data subjects.¹⁰

⁸ UK reservation: UK thought this should not be set out in the Regulation. FR and LT sought clarification on the scope of the data protection by design and by default and on why the processor was not included.

⁹ DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. This debate will however need to take place in the context of a debate on pseudonymising personal data.

¹⁰ SI thought that it would be better to change the sequencing of the text to mention rights first and then available technology; focus should be on individuals' rights and that costs and technology should be adapted to these rights.

2. The controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are **necessary**¹¹ 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.
- 2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.
3. (...)
4. (...)

¹¹ BE and CZ would prefer "not excessive". This term may be changed again in the future in the context of the debate on the wording of Article 5(1)(c).

Article 24

Joint controllers¹²

1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They 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. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.
2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (...) controllers.
3. **Paragraph 2 does not apply in case the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights (...).**

¹² EE scrutiny reservation. SI and UK reservation: UK thought this provision should be deleted. UK and ES thought this article does not take sufficiently account of cloud computing. CZ and DE expressed grave doubts about the enforceability of this provision in the private sector outside arrangements within a group of undertakings. CZ and DE thought this article should contain a safeguard against outsourcing of responsibility. FR thought the allocation of liability between the controller and the processor is very vague. DE and RO emphasised that it would be in the interest of the data subject to have clear rules and thought the article should therefore be clarified. Other delegations (DK, EE, SE, SI and UK) warned against potential legal conflicts on the allocation of the liability.

Article 25

Representatives of controllers not established in the Union¹³

1. Where Article 3(2) applies; the controller shall designate in writing a representative in the Union¹⁴.
2. This obligation shall not apply to:
 - (a) (...) ¹⁵; or
 - (b) processing which is unlikely to result in a high risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing (...) ¹⁶; or

¹³ DE, GR and UK scrutiny reservation. Several delegations (DE) expressed doubts as to whether the tool of obliging controllers not established in the EU to appoint representatives was the right one to ensure the application of EU data protection law to the offering of services and goods in the EU, in view, inter alia, of the low success of this tool under the 1995 data protection directive. CZ and UK also questioned the enforceability of this provision and thought it should be considered alongside Article 3(2). BE, DE FR, IT, PL and UK argued that, if such obligation were to be imposed, the Regulation, Article 79(6)(f) of which provides a mandatory fine for failure to appoint a representative, should clearly allocate duties and tasks to the representative. Reference was also made to the lack of clarity regarding possible sanctions in case of non-designation of a representative. FR also thought the representative's contact details should mandatorily be communicated to the DPA and referred specifically to the potentially problematic case of non-EU air carriers which, often in cooperation with EU carriers, offered flights to EU residents and might not have a representative in the Union.

¹⁴ SI reservation.

¹⁵ Deleted further to BE, DE, PL, SI and SK reservation. COM confirmed that this indent also covered the Safe Harbour Agreement and pointed out that under Article 41(2)(1) of its proposal having effective and enforceable rights was precisely one of the determining elements to be taken into account in the case of an adequacy decision.

¹⁶ The SME-exemption was deleted further to the remarks by BE, DE, ES, FR, FI, GR, HU, IT, LT, LV, PL, PT, SI and SK, which stated that the SME-criterion in itself, while being relevant, could not be sufficient to determine the applicability of the obligation to appoint a representative. The risk inherent in data processing operations should be more important and this text proposal seeks to incorporate this element. DE, FR and HU remarked that the proposed criterion itself would exclude 99.8 % of all enterprises in third countries from the scope of this obligation. COM, UK, supported by CZ and EE, wanted to keep the SME exception in the text to protect SME for economic burdens; it indicated that the exemption did not unduly restrict the obligation to designate a representative.

- (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.

Article 26

Processor

1. (...).¹⁷ The controller shall use only processors providing sufficient guarantees¹⁸ to implement appropriate technical and organisational measures (...) in such a way that the processing will meet the requirements of this Regulation (...).

¹⁷ At the suggestion of several delegations the phrase "Where personal data are processed on behalf of the controller, the controller shall be responsible for ensuring compliance with data protection rules." was deleted. The Presidency suggest completing Article 5(2) with the words "also in case of personal data being processed on its behalf by a processor".

¹⁸ DK, RO and HR thought the 'sufficient guarantees' should be detailed.

- 1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes¹⁹.
- 1b. (...) ²⁰.
2. The carrying out of processing by a processor shall be governed by a contract or a 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 the controller (...) and stipulating, 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 before processing the data, unless that law prohibits such information on important grounds of public interest²¹;
- (b) (...)
- (c) take all (...) measures required pursuant to Article 30;

¹⁹ LU and FI were concerned that this might constitute an undue interference with contractual freedom.

²⁰ Several delegations (BE, CZ, DK, AT, LU) pointed to the need to align this with the rules in Article 77. The discussion on the exercise of data subjects rights should indeed take place in the context of Chapter VIII.

²¹ Several delegations (ES, FR, PT) were concerned about the possibility for Member State law to restrict the possibility of prohibiting such notification. HR thought this could be allowed only in case it explicitly prohibits and FI suggested that the controller should be informed thereof beforehand. BE queried what would happen in case a non-EU law imposed such obligation. However, the Presidency informs that EU law also contains such requirements (e.g. in the context of the fight against money laundering).

- (d) ²²respect the conditions for enlisting another processor (...), such as a requirement of specific prior permission of the controller²³;
- (e) (...) 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) (...) 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 services²⁴ 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 subject²⁵;
- (h) make available to the controller (...) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller.

The processor **shall** immediately inform the controller if, in his opinion, an instruction breaches **applicable law**.

²² UK thought this overlapped with other parts of the Regulation (Article 26,(2)(a) and 30. AT and SK scrutiny reservation.

²³ BE, supported by ES, had suggested to draw inspiration from Article 11(1) of Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC. HR wanted to move the paragraph to paragraph 2a.

²⁴ BE: the word "completion" is not the best option since the duty should also apply in case of the contract is terminated before the completion of the processing specified in the contract. The new proposed wording comes from clause 12 of Model clause 2010/87/UE and has been therefore commonly agreed in Committee 31.

²⁵ BE suggested adding 'and will not actively process the personal data transferred anymore'; the duty to respect security measure being a at any rate applicable. It also suggested reintroducing 'in that case the processor shall implement appropriate measures to ensure the security and confidentiality of the personal data'.

2a. Where a processor enlists (...) 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 *by way of a contract or other legal act under Union or Member State law*²⁶, 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 obligations²⁷.

2aa. *Adherence of the processor to a code of **an approved** conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39*²⁸ may be used as an element to demonstrate *sufficient guarantees referred to in paragraphs 1 and 2a.*

²⁶ HU suggested qualifying this reference to EU or MS law by adding "binding that other processor to the initial processor".

²⁷ BE suggested adding an obligation for the processor not to enlist another processor without the prior specific or general written consent of the controller. In the latter case, BE thinks that the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.

²⁸ FR reservation; BE and SK suggested specifying that where the other processor fails to fulfil its data protection obligations under such contract or other legal act, the processor shall remain fully liable to the controller for the performance of the other processor's obligation. By authorising the processor to subcontract itself and not obliging the subprocessor to have a contractual relationship with the controller, it should ensure enough legal certainty for the controller in terms of liability. The principle of liability of the main processor for any breaches of subprocessor is provided in clause 11 of Model clause 2010/87 and BCR processor and is therefore the current standard. It also suggested deleting the reference to Article 2aa.

- 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 part, 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 39a²⁹.
- 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)³⁰.
- 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. (...)³¹

Article 27

Processing under the authority of the controller and processor

(...)³²

²⁹ IE reservation.

³⁰ PL was worried about a scenario in which the Commission would not act. CY and FR were opposed to conferring this role to COM (FR could possibly accept it for the EDPB).

³¹ COM reservation on deletion.

³² ES, FR, SI and UK stated that it is difficulty to see what is the added value of this Article as compared to Article 26, §2(b). As for employees of the controller, the latter will always be liable for any data protection violations carried out by the former. All confidentiality duties have now been moved to Article 30.

Article 28

Records³³ of categories of personal data processing activities³⁴

1. Each controller (...) ³⁵ 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) ³⁶;
 - (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 (...) ³⁷;
 - (g) where possible, the envisaged time limits for erasure of the different categories of data.

³³ 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.

³⁴ 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. NL and SE shared these concerns.

³⁵ Several delegations (BE, DE) thought the processor should not have cumulative obligations with the controller. ES and UK pointed out that the impact of cloud computing needed further reflection.

³⁶ UK suggested deleting it, as it overlaps with Article 6(1)(f).

³⁷ UK reservation.

- (h) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).
- 2a. Each processor³⁸ 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;
- (e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).
- 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 authority³⁹.
4. The obligations referred to in paragraphs 1 and 2a shall not apply to:
- (a) (...); or
- (b) (...) ⁴⁰; or

³⁸ UK thinks this article should not apply to processors at all, as all their processing activities are carried out under the responsibility of the controller.

³⁹ SI wondered why the data subject was not mentioned here. COM stated this information of the data subject is covered by the general principles. FI proposed to insert an exception in case the controller is subject to a professional secrecy duty, but this is already covered by Article 84 of the regulation.

⁴⁰ Deleted further to the criticism of AT, BE, DE, DK, ES, FR, GR, IT, LT, LU, NL, MT, PT.

- (c) categories of processing activities which⁴¹ by virtue of the nature, context, scope or purposes of the processing are unlikely to result in a **high** risk for the rights and freedoms of **individuals**, such (...) **discrimination, identity theft or fraud[, breach of (...) pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing.**
5. (...)
6. (...)

Article 29

Co-operation with the supervisory authority

(...)

⁴¹ Proposal inspired by Article 18(2) of the Data Protection Directive, in order to take account of delegations that thought that the proposed exceptions were not well-founded and that risk-based exceptions would be preferable. FR thinks that the risk-based approach cannot lead to exemption of certain types of processing operations.

SECTION 2

DATA SECURITY

Article 30

Security of processing⁴²

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of **individuals**, the controller and the processor shall implement appropriate technical and organisational measures, including (...) [pseudonymisation] of personal data to ensure a level of security appropriate to the risk.
 - 1a. In assessing the appropriate level of security account shall be taken in particular of the risk that are presented by data processing (...), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
 2. (...)
 - 2a. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 **may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.**
 - 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. (...)

⁴² DE indicated it would want to have a clause allowing specific rules for the public sector.

Article 31

Notification of a personal data breach to the supervisory authority⁴³

1. In the case of a personal data breach which is likely to result in a **high** risk for the rights and freedoms of **individuals**, such as discrimination, identity theft or fraud, financial loss, [breach of (...) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, 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.
 - 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)⁴⁴.
2. (...) The processor shall notify the controller without undue delay after becoming aware of a personal data breach⁴⁵.
3. The notification referred to in paragraph 1 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;

⁴³ AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.

⁴⁴ BE, DE, AT and PL thought this paragraph should be deleted.

⁴⁵ DE remarked that in view of the Commission proposal of 7 February 2013 for a Directive concerning measures to ensure a high level of network and information security across the Union (COM(2013) 48 final), it should be checked whether in certain cases the authority competent for network and information security should also be notified.

- (c) (...)
 - (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, comprising the facts surrounding the breach, its effects and the remedial action taken⁴⁶. This documentation must enable the supervisory authority to verify compliance with this Article. (...).
5. (...)
6. (...)⁴⁷

⁴⁶ AT, LU and FR queried what was the retention period for this documentation.

⁴⁷ COM reservation on deletion.

Article 32

*Communication of a personal data breach to the data subject*⁴⁸

1. When the personal data breach is likely to result in a **high** risk for the rights and freedoms of **individuals**, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (...) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall (...) ⁴⁹ communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (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 (...) ⁵⁰ has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

⁴⁸ 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.

⁴⁹ 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'

⁵⁰ NL and FR criticised the subjective criterion of satisfying to the satisfaction of the DPA. More generally, NL opined that there was danger of the data protection authority would obtain company secrets from the data controller which the DPA might be obliged to disclose under access to document legislation.

- b. the controller has taken subsequent measures which ensure that the **high** risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; 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 interest⁵¹.
4. (...)
5. (...)
6. (...)⁵²

⁵¹ HR suggested adding a qualification that this public interest is recognised in (Union or MS) law. The Presidency thinks this is implicit and therefore redundant. In not other instance (except Chapter V) this has qualification has been made.

⁵² COM reservation on deletion.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 33

*Data protection impact assessment*⁵³

1. Where **a new type of** processing, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high⁵⁴ risk for the rights and freedoms of **individuals**⁵⁵, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (...) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller (...)⁵⁶ shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (...)⁵⁷.
 - 1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

⁵³ DE, HU scrutiny reservation; FR thought that the possible application to public/private archives required further scrutiny. FR said that both Articles 33 and 34 raised problems for FR; as it wanted all processing to be subject to an impact assessment.

⁵⁴ FR, PT, RO, SK, SI and UK warned against the considerable administrative burdens flowing from the proposed obligation.

⁵⁵ BE and RO scrutiny reservation.

⁵⁶ COM reservation on deletion.

⁵⁷ ES had proposed exempting certified processing operations. BE, CZ, EE and had proposed exempting a controller who had appointed a DPO.

2. A data protection impact assessment referred to in paragraph 1 may in particular be required in the following cases:
- (a) a systematic and extensive evaluation (...) of personal aspects relating to (...) natural persons (...), which is based on profiling and on which decisions⁵⁸ 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)(...)⁵⁹, biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (...) decisions regarding specific individuals on a large scale ;
 - (c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (...)⁶⁰;
 - (d) (...);
 - (dd) (...);
 - (de) (...);
 - (e) (...)⁶¹.

⁵⁸ 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. FR thought profiling measures might need to be covered by this Article, but this type of processing is largely covered by paragraph 2(a). The Presidency proposes that this wording b aligned to the eventual wording of Article 20 and has therefore bracketed this language

⁵⁹ HU suggested that data pertaining to children be also reinserted.

⁶⁰ BE, DE, FI, FR, FI, AT, SK asked for the deletion or better definition of 'large scale'. COM referred to recital 71.

⁶¹ BE, FR, IE scrutiny reservation; BE and DE reservation: in favour of deleting this subparagraph. NL and PL thought a role could be given to the EDPB in order to determine high-risk operations.

- 2a. The supervisory authority shall establish and make public a list of the kind of processing operations 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.⁶²
- 2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.
- 2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve 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.⁶³
3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1, the measures envisaged to address the risk 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 concerned⁶⁴.

⁶² CZ, EE, NL, SI and DE reservation. NL suggests deleting this. HU wondered what kind of legal consequences, if any, would be triggered by the listing of a type of processing operation by a DPA with regard to on-going processing operations as well as what its territorial scope would be. In the view of the Presidency any role for the EDPB in this regard should be discussed in the context of Chapter VII.

⁶³ CZ, EE, NL, SI and DE reservation. NL suggests deleting this 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.

⁶⁴ 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.'

- 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 assessment⁶⁵.
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.⁶⁶
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 question⁶⁷, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities⁶⁸.
6. (...)
7. (...)

⁶⁵ HU thought this should be moved to a recital. IE scrutiny reservation.

⁶⁶ BE, FR indicated that this was a completely impractical obligation.

⁶⁷ BE reservation; it suggested this qualification be deleted.

⁶⁸ DK 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. DE 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).

Article 34

Prior (...) consultation⁶⁹

1. (...)
2. The controller (...) ⁷⁰ 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 **would** result in a high (...) risk **in the absence of measures to be taken by the controller to mitigate the 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 controller has insufficiently identified or mitigated the risk, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may prohibit the processing pursuant to Article 53, paragraph 1b, letter e)⁷¹. 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 delay⁷².
4. (...)
5. (...)

⁶⁹ HU, RO and UK scrutiny reservation; SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

⁷⁰ COM and LU reservation on deleting processor.

⁷¹ IE and UK scrutiny reservation.

⁷² SI scrutiny reservation.

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 (...).
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 (...) ⁷³.
- 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 ⁷⁴.
8. (...)
9. (...)

⁷³ IE scrutiny reservation on deletion.

⁷⁴ DK, NL, SE and SI scrutiny reservation.

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,⁷⁵ designate a data protection officer (...).
2. A group of undertakings may appoint a single data protection officer.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. (...).
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. (...).
6. (...)
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.

⁷⁵ Made optional further to decision by the Council. DE and AT scrutiny reservation. DE, HU and AT would have preferred to define cases of a mandatory appointment of DPA in the Regulation itself. COM reservation on optional nature and deletion of points a) to c). UK thinks paragraphs 5 to 8 could be deleted.

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.
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 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. (...)

Article 36

Position of the data protection officer⁷⁶

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.

⁷⁶ UK thought articles 36 and 37 could be deleted in a pure risk-based approach.

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 interests⁷⁷.

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

⁷⁷ Moved from Article 35 (6). DE was opposed to this as these requirements were irrelevant to the functional independence of the DPO. FR demanded further clarifications. UK also thought this was too prescriptive. This paragraph was redrafted in order to make it less prescriptive. AT thought the redraft did not sufficiently take account of the situation of external DPOs.

- (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 referred to in Article 34, and consult, as appropriate, on any other matter.

2. (...)

2a. The data protection officer shall **in the performance** his tasks have due regard to the risk associated with the processing operations, taking into account the purpose, nature and context of the processing.

SECTION 5

CODES OF CONDUCT AND CERTIFICATION⁷⁸

Article 38

Codes of conduct^{79 80}

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.

⁷⁸ COM scrutiny reservation on Section 5.

⁷⁹ AT, DK, FI, SK and PL scrutiny reservation. DE, FR and SI stated that this article should not apply to the public sector.

⁸⁰ Several delegations thought more incentives should be made to apply to the use of codes of conduct: BE, DE, DK, LV, SE, SI, UK. Several delegations thought that hortatory language was being used in §1 (SI, PT), §1c (NL, SI, FR).

1a. Associations and other bodies representing categories of controllers or processors 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;
- (b) the collection of data;
- (bb) the pseudonymisation of personal data;
- (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;
- (ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;
- (f) (...).

1ab. **In addition to adherence by controller or processor subject to the regulation,** codes of conduct may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall take binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights.

- 1b. Such a code of conduct shall contain mechanisms which enables the body referred to in paragraph 1 of article 38a to carry out the mandatory⁸¹ monitoring of 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 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 and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards⁸².
- 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 is approved, and if 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 draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.
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, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission⁸³.

⁸¹ CZ preferred this monitoring to be optional.

⁸² 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 (4) of this Regulation.

⁸³ DE, IE, ES, PT also remarked that the DPAs should be involved; to that end paragraph 2a has been inserted. EE, ES and UK thought that the Commission need not be involved.

4. The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union⁸⁴. 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 approved codes which have been decided as having general validity in accordance with paragraph 4⁸⁵.
- 5a. The European Data Protection Board shall collect all approved codes of conduct **and amendments thereto** in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal .

Article 38a

Monitoring of approved codes of conduct⁸⁶

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 body⁸⁷ 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.

⁸⁴ EE and FR queried what was the legal status of such approved codes of conduct and in particular their binding nature.

⁸⁵ BG suggests deleting paragraph 4; ES suggests deleting paragraphs 4 and 5.

⁸⁶ AT, DE , DK, LU, NL, FI and UK scrutiny reservation.

⁸⁷ CZ, DK, EE, ES, LV, LU PT and UK are opposed to giving this role to such separate bodies. Concerns were raised, *inter alia*, on the administrative burden involved in the setting up of such bodies. Codes of conduct are an entirely voluntary mechanism in which no controller is obliged to participate.

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;
 - (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 Regulation⁸⁸.

⁸⁸ BE proposed adding: 'An infringement of a code of conduct shall not in itself constitute an infringement of this Regulation, unless the Commission has, pursuant to paragraph 4 of Article 38, decided the code has general validity within the European Union.' This proposal should be revisited in the wider context of the discussions on sanctions.

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

Article 39

Certification⁸⁹

1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at **Union** level, the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.
- 1a. **In addition to adherence by controller or processor subject to the regulation, data protection certification mechanisms, seals or marks may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall take binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights.**
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.

⁸⁹ AT, DK, EE, FR, FI and UK scrutiny reservation. ES, SI and UK thought further incentives should be provided for using certification mechanism. FR thought the terminology used was unclear and that the DPA should be in a position to check compliance with certified data protection policies; this should be clarified in Article 53.

- 2a. A certification pursuant to this Article shall be issued by the accredited bodies referred to in Article 39a, or where applicable, by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board⁹⁰.
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 shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by **the accredited bodies referred to in Article 39a, or where applicable, the competent supervisory** authority where the requirements for the certification are not or no longer met.
5. The European Data Protection Board shall collect all **certification mechanisms and data protection seals** in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

⁹⁰ This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

Article 39a

Certification body and procedure⁹¹

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall⁹² be issued and renewed by:
 - (a) 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; or
 - (b) **the National Accreditation Body named in accordance with Regulation (EC) 765/2008 in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a**⁹³.

2. The body referred to in point (a) of paragraph 1 may be accredited for this purpose only 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;
 - (aa) (...) ⁹⁴.
 - (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;

⁹¹ AT, DK, EE, FR, LU and SI scrutiny reservation.

⁹² UK thought this should be "may".

⁹³ ES proposal

⁹⁴ Moved to paragraph 5.

- (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 **point (a)** of paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.
4. The bodies referred to in **points (a) and (b)** of 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. The accreditation is issued for a maximum period of [five years] and can be renewed in the same conditions as long as the body meets the requirements.
5. The bodies referred to in **points (a) and (b)** of paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification. *They shall undertake to respect the criteria elaborated by the competent supervisory authority or the European Data Protection Board⁹⁵ as referred to in paragraph 2a of Article 39.*
6. **In case of an accreditation pursuant to point (b) of paragraph 1, the competent supervisory authority under Articles 51 or 51a may establish specific requirements that complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the Certification bodies. *These criteria, the criteria referred to in paragraph 2a of Article 39 and the certification details shall be made public by the supervisory authority in an easily accessible form.*** The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect criteria for certification and the certification details in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.

⁹⁵ This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

- 6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority shall revoke the accreditation of a body referred to in **point (b) of 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.
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 7⁹⁶.
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)⁹⁷.

⁹⁶ This is without prejudice to the future discussion on the exact powers of the EDPB. This discussion will take place in the context of the discussion on the one-stop-shop mechanism.

⁹⁷ DE pleaded in favour of deleting the last two paragraphs and suggested adding a new paragraph: "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." ES also thought that this should not be left exclusively to the Commission.