Council of the European Union

Brussels, 1 August 2014
(OR. en)

12312/14

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:	Working Party on Information Exchange and Data Protection
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 are 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 were invited to send in written comments. The Presidency thanks delegations for the many useful comments it received from delegations[1].

---

[1]   12267/14 DATAPROTECT 107 JAI 625 MI 574 DRS 102 DAPIX 107 FREMP 146 COMIX 395 CODEC 1671

3.   Further to these comments the Presidency has made further changes to Chapter IV. It 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. Some of the outstanding issues are further explained out hereafter.

Risk concept

4.   Regarding the risk concept referred to in Article 22 and recitals 60, several delegations were of the opinion that this should be further detailed[2]. Other delegations indicated that it would be difficult to arrive at a definition that would stand the test of time and warned against 'cataloguing' different types of risk[3]. Some thought that a description or definition of low risk should also be given, but this was not supported by the majority of delegations.

5.   Several delegations have rightly pointed to the need to have a more consistent and systematic terminology regarding risk. The Presidency has therefore tried to redraft Chapter IV in order to distinguish three different levels of risk. In doing so, it has also endeavoured to align the language throughout the text.

General concept of risk:

6.   As indicated in the 'horizontal clause' of Article 22 (and other articles of Chapter IV), the risk refers to risks to rights and freedoms of data subjects. Recital 60 has been supplemented to clarify that risks are all situations that might prejudice the rights and freedoms of data subject and the Article 22 has been supplemented by the reference to the likelihood and severity of the risk, which was already contained in recital 60.
Recital 60 gives a list of examples, what could be seen as situations, which present any kind of risk. It has rightly been stated by delegations that there is no zero risk. The general risk notion is mentioned in several articles (e.g. art 22, 23, 30).

---

[2]   DE, ES, HU, NL, PT, FI and RO.
[3]   IE and COM.

High (or specific) risk

7. In one case the Regulation imposes duties on the controller which are triggered by an increased level of risk, namely to conduct impact assessment (Article 33). In two other cases the presence of an increased level of risk serves as an exception to the so-called SME exemption: SMEs are nevertheless obliged to comply with the obligations (appointing a representative (Article 26) and maintaining records (Article 28)) of which they are otherwise exempted.

8. Previous versions of the text of the Regulation referred to 'specific' risks in Articles 26, 28, and 33. The NL delegation has proposed to refer to 'high' risk. Whilst the exact terminology is not crucial, the Presidency thinks that the term 'high degree of risk' better encapsulates the idea of an increased level of risk. Various forms of data processing may present risks that are specific to these forms of processing, without necessarily representing a higher form of risk. The various articles mentioned (26, 28 and 33) now all refer to a 'high degree of risk'. The text of recital 67 has also been amended to better express the idea of a high degree of risk and Article 33(1) has been expanded to clarify the concept.

9. Article 33(1) contains a number of examples of high-risk operation which necessitate a DPIA. In this regard the suggestion for referring to the legitimate expectations of data subjects as a criterion instead of the reference in Article 33(2)(b) to 'large-scale', was not met with approval by the majority of delegations. Nevertheless delegations acknowledge that some controllers, by the very nature of their professional activities, (such as doctors, hospitals, attorneys, etc.) in certain cases be expected to process sensitive data on a large scale, without this justifying a DPIA. The Presidency therefore suggests (1) referring to 'processing reasonably likely to take place in the context of the processing operation' and (2) has sought to clarify the reference to 'other operations where the competent supervisory authority considers that the processing is likely to result in high degree of risks for the rights and freedoms of data subjects'.

Very high risk:

10. In two cases the Regulation imposes duties on the controller which are triggered, not just by an increased, but by a very high level of risk; namely data breach notification (Articles 31 and 32) and data protection impact assessment (DPIA) (Article 33). Regarding data breach notification the Regulation used the phrase 'severely affect' rights and freedoms of data subjects'. Data breach notification was indeed one of the items on which the Irish Presidency incorporated a strong risk-based approach, which was confirmed at last DAPIX meeting

11. Regarding the prior consultation, it was stated that this was required in case of high degree of specific risk. Several delegations have underscored the causal link between the data protection impact assessment (DPIA) described in Article 33 and the prior consultation in Article 34. The latter is triggered only when the degree of risk which necessitated the DPIA cannot be mitigated by certain measures from the controller. Previously a degree of risk which necessitated the DPIA was described as 'specific risks', whereas the prior consultation was required in case of high degree of specific risk. As the Presidency has now proposed to use the term 'high degree of risk' for the level of risk which triggers a DPIA, its is suggested to refer to a 'very high degree of for those cases in which the DPA needs to be consulted.

Consultation or authorisation

12. Currently the text of Article 34 provides no sanction in case of failure on behalf of the controller to consult the data protection authority or to follow its advice, even though Article 79(3), letter (i) provides for an administrative sanction in case of failure to consult the data protection authority. Recital 74 also clarifies that the lack of a reaction within this period is without prejudice to any later intervention of the supervisory authority. At the DAPIX meeting on 10-11 July 2014 a majority of delegations appeared to be opposed to prohibiting processing operations pending the opinion of the data protection authority

13. NL has made a text proposal, which is presented in the annex as an alternative version for Article 34 and recital 74, in which it suggests to turn the consultation procedure into an 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. According to NL, its proposal also has the advantage of allowing data protection authorities to draw a clear line between informal talks and the use of formal powers, which is important for their procedural position in subsequent court cases.

14. The Dutch proposal also builds on the on the two-step approach, namely that the existence of an increased level of risk must first be assessed by the controller (on the basis of a "reasonableness test" which is in the domain of his responsibility, pursuant to Article 22). Only if the outcome of the data protection impact assessment is that the existence of a high risk cannot be mitigated by reasonable measures in terms of available technology and costs, according to the controller, should the controller request an authorisation by the data protection authority.

15. 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. Also the French delegation has pleaded in favour of binding DPA decisions and at the DAPIX meeting on 10-11 July 2014 a minority of Member States lent their support to the idea of prohibiting processing operations for which the data protection authority has rendered a negative opinion.

Liability of processors and controllers

16. Several delegations highlighted the need to study the general question of responsibility for processing (and in particular the way it is to be applied by the phenomenon of cloud computing). Delegations have emphasised the need for a horizontal discussion on this topic, by including, inter alia, the DPA powers. The current version of Article 77 allows for both the controller and processor to be held liable for data protection violations and Article 79 allows for administrative fines against controllers and, in many cases, also against processors The question whether the respective liability of controllers and processors requires further adjustments in Chapter IV will therefore need to be discussed in the context of Chapter VIII and the Presidency will ensure that any decision to 'close' Chapter IV is without prejudice to later possibilities.

17. *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 various levels of risk as set out above;*

    ✓ *confirm the consultation procedure or indicate whether it should be replaced by an authorisation procedure;*

    ✓ *discuss all articles of Chapter IV on an article-by-article basis.*

_____

60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. **Risks should be evaluated on an objective assessment, by which its established whether data processing is likely to prejudice the rights and freedoms of data subjects.**[4] Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:

- o where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage; or
- o where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- o 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;
- o 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;
- o where personal data of vulnerable individuals, in particular of children, are processed;
- o where processing involves a large amount of personal data and affects a large number of data subjects[5].

---

4   Further to EE proposal to clarify the general notion of risk.
5   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'.

60a) (…)

60b) (…)

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

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

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

63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour in the Union, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise <u>unless the processing it carries out involves **a high degree of risk** for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing</u> or is a public authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.

<u>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.</u>

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

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

64) (…)

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

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

66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the (…) risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **risks that are presented by data processing, such as** accidental or **unlawful** destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, **which may in particular lead to physical, material or moral damage**[6].

67) A personal data breach may, if not addressed in an adequate and timely manner, result in severe **physical**[7], material or moral harm to individuals such as loss of control over their personal data or limitation of (…) their rights, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. **These cases with a high degree risk are situations, where based on an objective assessment, it is established whether data processing is likely to severely prejudice the rights and freedoms of data subjects.**[8] Therefore, as soon as the controller becomes aware that (…). a personal data breach **which may result in severe physical, material or moral harm** has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose ~~personal~~ rights and freedoms could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. (…).

---

6   Further to EE proposal to create a link to the recital 60, which explains the general notion of risk.
7   EE proposal to align the wording to that of recital 60.
8   Further to EE proposal.

The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example (…) the need to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

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

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

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

70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those processing operations which are likely to present high risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes and context (…). In such cases, a data protection impact assessment should be carried out by the controller (…) prior to the processing in order to assess the severity and likelihood of these **high** risks, taking into account the nature, scope**, purposes and context**[9] of the processing and the sources of the risks, which should include in particular the envisaged measures, safeguards and mechanisms for mitigating those risks and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to **(…)** large-scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects **and** which are particularly **invasive**, for example, on account of their **sensitivity**, where [**in accordance with the achieved state of technological knowledge**[10]] a new technology is used **on a large scale as well as to other processing operations which present a high degree of risks for the rights and freedoms of data subjects, in particular** where it is more difficult for data subjects to exercise their rights[11].
The processing of a considerable amount of personal data, also of sensitive data, should not be considered as being on a large scale, if the processing of these data is necessary for but does not constitute the core professional activities of the controller, such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney.

---

9 NL proposal.
10 SK proposal.
11 Further to proposal by DE.

ALTERNATIVE:

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

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

74) Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a **very** high degree of risks to the rights and freedoms of data subjects, such as **substantial loss of control over their personal data or significant limitation of**[12] their rights or giving rise to a disproportional invasion of privacy , unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of the processing activities. **Such very high degree of risk is presented by certain type of data processing and certain extent and frequency of processing, which may result in a realisation of extensive damage or disproportionate harm to rights and freedoms of data subject**[13]**.** The supervisory authority should give advice where the envisaged processing might not be in compliance with this Regulation. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation[14]. Such consultation should equally take place in the course of the preparation of a legislative or regulatory measure which provide for the processing of personal data.

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

---

[12]   EE proposal.
[13]   Further to EE proposal to link the concept of very high degree of risk to the notion of „severely affect" as well as the notion „high risks", which are listed as examples in article 33(2) taking into account the type of data (i.e. sensitive data) as well as the extent/frequency of the processing (i.e. systematic and extensive; on a large scale etc.).
[14]   The Presidency draws delegations attention to the fact that these powers under Article 53 include the power to prohibit certain processing operations.

ALTERNATIVE: Where a data protection impact assessment indicates that the processing is likely to present, despite the envisaged safeguards, security measures and mechanisms to mitigate the risks, a **very** high degree of **residual** risks to the rights and freedoms of data subjects, such as **substantial loss of control over their personal data or significant limitation of**[15] their rights or giving rise to a disproportional invasion of privacy , unlawful or arbitrary discrimination, substantial identity theft, significant financial loss, significant damage of reputation or any other significant economic or social damage, or by the use of specific new technologies, **the data controller should apply for an authorisation with the supervisory authority** (...) prior to the start of the processing activities. **Such very high degree of risk is presented by certain type of data processing and certain extent and frequency of processing, which may result in a realisation of extensive damage or disproportionate harm to rights and freedoms of data subject**[16]**. The supervisory authority should be competent to issue a permanent, temporary or conditional authorisation, if it finds the risks can not be mitigated by reasonable measures in terms of available technology and costs of implementation to be taken by the controller .** (...) **The supervisory authority should be competent to refuse the authorisation if the risks can not be mitigated or the processing operations would otherwise not be in compliance with the Regulation.** The supervisory authority should respond to **an application** (...) within a defined period (…).

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

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

---

15   EE proposal.
16   Further to EE proposal to link the concept of very high degree of risk to the notion of „severely affect" as well as the notion „high risks", which are listed as examples in article 33(2) taking into account the type of data (i.e. sensitive data) as well as the extent/frequency of the processing (i.e. systematic and extensive; on a large scale etc.).

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

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

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

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

CHAPTER IV

CONTROLLER AND PROCESSOR[17]

SECTION 1
GENERAL OBLIGATIONS

Article 22

__Obligations__ of the controller[18]

1.   Taking into account the nature, context, scope and purposes of the processing **as well as the likelihood and severity of**[19] risk for the rights and freedoms of data subjects, the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[20].

---

[17]   DK, PT, SI and UK scrutiny reservation on the entire chapter. BE stated that it was of the opinion that the proposed rules, while doing away with the general notification obligation on controllers, did not reduce the overall administrative burden/compliance costs for controllers. The Commission disagreed with this. DE, DK, NL, PT and UK were not convinced by the figures provided by COM according to which the reduction of administrative burdens outbalanced any additional burdens flowing from the proposed Regulation. FR referred to the impact this article should have on members of the professions (*professions libéraux*) who collect sensitive data as part of their work (e.g. health professionals).

[18]   DE scrutiny reservation. UK thought this Article could be deleted as it overlaps with existing obligations. UK thought it focuses too much on procedures rather than on outcomes. DE, LT and PT deplored that Article 22 does not contain an exception for SMEs. BE remarked that anyone who puts a photo on social media might be considered as a controller. SK proposed introducing a new concept of 'entitled person' in Article 4, together with obligations for the controller and processor to instruct their 'entitled persons' who come into contact with personal data about rights and obligations under this regulation as well as laying down responsibility for their infringement.

[19]   CZ proposal to align the text to that of recital 60.

[20]   BE and UK referred to the danger in maintaining such a vaguely worded obligation, applicable to all controllers, non-compliance of which is liable to sanctions.

---

2.   (…)[21]

2a.   Where proportionate in relation to the processing activities[22], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller[23].

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

3.   (…)

4.   (…)

---

[21]   PL asked for the reinstatement of this paragraph.
[22]   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.
[23]   UK thought this was too complicated. ES thought the concept of 'appropriate data protection policies' was too vague.

Article 23

Data protection by design and by default[24]

1.   Having regard to <u>available technology</u> and the cost of implementation <u>and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing,</u> the controller shall (…), implement (…) technical and organisational measures <u>appropriate to the processing activity being carried on and its objectives, including pseudonymisation of personal data,</u> in such a way that the processing will meet the requirements of this Regulation and <u>protect</u> the rights of (…) data subjects.[25]

2.   The controller shall implement <u>appropriate</u> <u>measures</u> for ensuring that, by default, only (…) personal data (…) which are **<u>necessary</u>**[26] for each specific purpose of the processing <u>are processed;</u> <u>this applies to</u> <u>the</u> amount of (…) data <u>collected,</u> the <u>period</u> of their storage <u>and their accessibility.</u> <u>Where</u> <u>the purpose of the processing is not intended to provide the public with information,</u> those mechanisms shall ensure that by default personal data are not made accessible <u>without human intervention</u> to an indefinite number of individuals[27].

---

[24]   UK reservation: UK thought this should not be set out in the Regulation. DE and FR scrutiny reservation; 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. DE and MT thought that more emphasis should be put on pseudonymising and anonymising data. 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. It also thought data protection by design and by default should be more used in response to risky data processing operations. ES thought that the term 'non-excessive data processing' was preferable to 'data protection by design'. FR also queried the exact meaning of the terms used in the title.

[25]   NL stated this paragraph added little in terms of legal obligations compared to other articles in the draft regulation. It might be moved to a recital.

[26]   IE suggestion.

[27]   DE and SE reservation; DE and UK queried the exact meaning of the last sentence for social media. SE thought this would be better moved to the recitals. BE and FR asked what this added to the principle of data minimisation contained in Article 5. AT thought the second sentence should be retained.

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

3.   (…)

4.   (…)

Article 24
Joint controllers [28]

1.   (…) Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. **The arrangement should designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights**[29]**.**

---

[28]   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, DE and NL 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 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. SE thought that the allocating respective liability between public authorities should be done by legislation. SI scrutiny reservation.

[29]   BE proposal. BE also suggested adding: The arrangement shall designate the supervisory authority in accordance with Article 51.' ES suggested adding ' For this agreement to be valid in relation to data subjects, it must be documented and must have been brought to their attention beforehand; otherwise, the aforementioned rights may be exercised in full before any of the controllers, and it shall be incumbent on them to ensure precise compliance with the legally established benefits.' SK also pleaded in favour of informing data subjects of any arrangements between several controllers.

---

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[30] unless the data subject has been informed in a transparent manner which of the joint controllers is responsible.

Article 25

Representatives of controllers not established in the Union[31]

1.   Where Article 3(2) applies, the controller shall designate in writing a representative in the Union[32].

---

[30]   DE, FR emphasised that it would be in the interest of the data subject to have clear rules which allow it to address its requests to all controllers concerned. Potential language problems in case of controllers established in different Member States were also highlighted. ES indicated that such arrangements can never be to the detriment of the data subject's rights and its proposal for paragraph 2 seeks to take account of the concerns.

[31]   DE, GR and UK scrutiny reservation. Several delegations (DE, NL, SE) 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.

[32]   SI reservation.

2.   This obligation shall not apply to:

    (a)   a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41[33]; or

    (b)   an enterprise employing fewer than 250 persons <u>unless the processing it carries out **presents a high degree of** risk for the rights and freedoms of data subjects, having regard to the nature, **context,** scope and purposes of the processing</u>[34]; or

    (c)   a public authority or body[35].

    (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[36].

---

[33]   BE, DE, NL, PL and SK reservation: they thought this indent should be deleted. At the request of several delegations, COM confirmed that this indent also covered the Safe Harbour Agreement. It also 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.

[34]   BE, DE, ES, FR, FI, GR, IT, LT,LV, PL, PT and SK remarked 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 remarked that the proposed criterion itself would exclude 99.8 % of all enterprises in third countries from the scope of this obligation.

[35]   SI thought this should be drafted more broadly so as to encompass any body which exercised sovereign governmental powers.

[36]   DE pointed out that paragraph 3 leaves it entirely up to businesses offering EU-wide internet services where they appoint a representative within the EU; it thought that this should be done in accordance with the rule on supervisory jurisdiction in the cases referred to in Article 3(2). At any rate, the supervisory authority in that Member State in which the representative is appointed should have jurisdiction.

3a.   The representative shall be mandated by[37] 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[38]

1.   (…)[39] The controller shall <u>use only</u> processor<u>s</u> providing sufficient guarantees[40] to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…).

---

[37]   BE proposed to state 'is liable'.
[38]   DE scrutiny reservation.
[39]   DE proposed starting the sentence by stating that the controller shall be responsible for ensuring compliance with data protection rules. Some delegations thought it should be explicitly stated that the rights of the data subject and the right to compensation for damages must be asserted against the controller.
[40]   BE, DK and HR thought the 'sufficient guarantees' should be detailed.

2.   The carrying out of processing by a processor shall be governed by a contract <u>or other legal act</u> **under Union or Member State law**[41] <u>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</u> (…) and stipulating<u>, in particular</u> that the processor shall:

(a)   process the personal data only on instructions from the controller (…)**[42]**, unless required to do so by Union or Member State law to which the processor is subject<u>; in such a case, the processor shall inform the controller of that legal requirement, unless that law prohibits such information on important grounds of public interest</u>[43];

(b)   (…)

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

(d)   [44]<u>respect the conditions for</u> enlis<u>ting</u> another processor (…), <u>such as a requirement of specific prior permission of the controller</u>[45];

---

[41]   AT suggested that the details referred to for the contract should also apply to 'other legal act'.

[42]   BE wants to underline the fact that this duty should not be only a contractual duty (as it is provided in art. 17(3) of Directive 95/46) but also a legal duty (as it is provided in art. 16 of directive 95/46) to enable not only data controller but also data subject to have redress mechanisms against the processor. Therefore, BE pleads for the reintroduction of art. 27 of draft regulation in order to avoid the current level of data protection to be diminished.

[43]   Further to PT suggestion. Several delegations (ES, FR, PT, SK) 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. BE queried what would happen in case a non-EU law imposed such obligation.

[44]   UK thought this overlapped with other parts of the Regulation (Article 26,(2)(a) and 30). DE thought the requirement should have been limited to establishment of contractual relationships. AT and SK scrutiny reservation: SK thought there were many questions surrounding the relation with this 'secondary' processor.

[45]   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.

(e)   as far as (…) possible, taking into account the nature of the processing[46], 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 services[47] specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject[48];

(h)   make available to the controller (…) all information[49] necessary to demonstrate compliance with the obligations laid down in this Article.

---

[46]   FR thought this was unclear and should possibly replaced by a reference to risk.

[47]   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.

[48]   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'.

[49]   DE referred to 'the principal's rights of supervision and the contractor's corresponding rights of tolerance and involvement', for instance rights of entry, certified auditor's obligations to report periodically.

2a. Where a processor enlists by way of a contract or other legal act **under Union or Member State law** another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations[50].

2aa. *The provision of sufficient guarantees referred to in paragraphs 1 and 2a may be demonstrated by means of adherence of the processor to a code of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39*[51].

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in parts, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a[52].

---

[50] 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.

[51] 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.

[52] IE reservation.

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) [53].

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.   (…)[54]

Article 27

Processing under the authority of the controller and processor

(…) [55]

---

[53]   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).
[54]   COM reservation on deletion.
[55]   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

Records[56] of categories of <u>personal data</u> processing activities [57]

1.   Each controller (…)[58] and, if any, the controller's representative, shall maintain <u>a</u> <u>record of</u> all <u>categories of</u> <u>personal data</u> processing <u>activities</u> under its responsibility[59]. [60]<u>This</u> <u>record</u> shall contain (…) the following information:

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

   (b)   (…)

   (c)   the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f)[61];

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

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

   (f)   where applicable, <u>the categories of</u> transfers of <u>personal</u> data to a third country or an international organisation (…)[62];

---

[56]   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.

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

[58]   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.

[59]   FR thought it should be specified for how long the documentation needed to be kept.

[60]   . NL thought the keeping of documentation should be made conditional upon a prior risk assessment: 'Where a data protection impact assessment as provided for in Article 33 indicates the processing operation presents a high degree of risk, referred to in Article 33'. RO is also in favour of a less prescriptive list.

[61]   UK suggested deleting it, as it overlaps with Article 6(1)(f).

[62]   UK reservation.

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

(h)   (…)

2a.   Each processor[63] shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:

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

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

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

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

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

3.   On request, the controller and the processor and, if any, the controller's representative, shall make the record available (…) to the supervisory authority[64].

---

[63]   UK thinks this article should not apply to processor(s at all, as all their processing activities are carried out under the responsibility of the controller.

[64]   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.

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

(a)   (…)[65]

[(aa)   controllers who have designated a data protection officer, pursuant to Article 35[66]];

(b)   an enterprise or a body employing fewer than 250 persons<u>, unless the processing it carries out **is likely to result in a high degree of risk** for the rights and freedoms of data subjects**, such as discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage for the data subjects**[67], having regard to the nature, **context,** scope and purposes of the processing[68]</u>; or

(c)   <u>categories of processing activities which[69] by virtue of the nature, **context,** scope or purposes of the processing are unlikely to **result in a high degree of risk** for the rights and freedoms of data subjects.</u>

5.   (…)

6.   (…)

---

[65]   COM reservation on deletion.
[66]   NL proposal. ES had previously made a similar proposal.
[67]   NL proposal.
[68]   Many delegations criticised the appropriateness of this criterion: AT, BE, DE, DK, ES, FR, GR, IT, LT, LU, NL, MT, PT, and SE. At the suggestion of BE, the criterion was narrowed in the same way as in Article 25(2)(b).
[69]   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.

Article 29

Co-operation with the supervisory authority

(…)[70]

SECTION 2
DATA SECURITY

Article 30

Security of processing[71]

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

1a. <u>In assessing the</u> **appropriate** <u>level of security account shall be taken in particular of the risks</u> **that are presented by data processing, which could lead to physical, material or moral harm, in particular**[72] <u>from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.</u>

2. (…)

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

---

[70] PT and ES scrutiny reservation on deletion.
[71] DE indicated it would want to have a clause allowing specific rules for the public sector.
[72] Further to EE proposal; see recital 78.

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

3. (…)

4. (…)

Article 31

Notification of a personal data breach to the supervisory authority[73]

1. In the case of a personal data breach which is likely to **present a high degree of risk for** the rights and freedoms of data subjects[74]**, such as discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage**[75], 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)[76].

2. (…) The processor shall alert and inform the controller without undue delay after becoming aware of a personal data breach[77] [78].

---

[73] AT and SI scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded.
[74] BE suggested adding: 'or creates a risk for the data subjects', which was opposed by CZ.
[75] NL proposal.
[76] BE thought that also point (a) of Article 32(3) should be added here. PL thought this paragraph should be deleted.

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

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

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

(c) (…)

(d) describe the <u>likely</u> consequences of the personal data breach <u>identified by the controller</u>;

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

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

3a. <u>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.</u>

4. The controller shall document any personal data breaches <u>referred to in paragraphs 1 and 2</u>, comprising the facts surrounding the breach, its effects and the remedial action taken[79].This documentation must enable the supervisory authority to verify compliance with this Article. (…).

---

[77] The Commission highlighted the importance of this obligation, in particular in the context of cloud computing. UK thought this should be moved to Article 26.

[78] 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.

[79] AT, LU and FR queried what was the retention period for this documentation.

5.   (…)

6.   **(….)**.[80]

Article 32

Communication of a personal data breach to the data subject[81]

1.   When the personal data breach is likely to **present a high degree of risk for** the rights and freedoms of data subjects[82]**, such as discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage**[83], severely affect the rights and freedoms of the data subject, the controller shall (…)[84] communicate[85] 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[86] 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).

---

[80]   BE, DE, IT, LT, RO and UK had pleaded for the deletion of paragraph 6. COM reservation on deletion.

[81]   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.

[82]   BE and SK scrutiny reservation. BE suggested adding: 'or creates a risk for the data subjects', which was opposed by CZ.

[83]   NL proposal.

[84]   AT, PT and SE clarified there is no valid reason why the data subject should always be informed after the DPA. Therefore this part has been deleted. DE however proposed to start this paragraph by stating: 'As soon as appropriate measures have been taken to render the data secure or where such measures were not taken without undue delay and there is no longer a risk for the criminal prosecution'

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

[86]   DE proposed adding "in generally comprehensible terms", but this is already covered by Article 12.

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

    a. the controller (…)[87] has implemented appropriate technological protection measures and (…) those measures were applied to the data <u>affected by</u> the personal data breach, <u>in particular those that</u>[88] render the data unintelligible to any person who is not authorised to access it<u>, such as encryption</u> **(…)**; or

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

    c. <u>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</u>

    d. <u>it would adversely affect a substantial public interest</u>[89].

4. (…)

5. (…)

6. **(…)**[90]

---

[87] 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.

[88] BE proposed 'have the purpose'.

[89] 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.

[90] BE, CZ, DK, DE, ES, PL and UK had pleaded for the deletion of paragraph 6. COM reservation on deletion.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment [91]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to **present a** high[92] **degree of** risk for the rights and freedoms of data subjects[93], **such as discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage**[94]*,* the controller **(…)**[95] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[96].

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

---

[91] DE, ES, 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.

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

[93] BE and RO scrutiny reservation.

[94] NL proposal.

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

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

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

    (a)   [a systematic and extensive evaluation (…) of personal aspects relating to (…) natural person<u>s</u> (…), which is based on <u>profiling</u> and on which <u>decisions</u>[97] are based that produce legal effects concerning <u>data subjects</u> or <u>severely</u> affect <u>data subjects</u>];

    (b)   <u>processing of special categories of personal data under Article 9(1)</u> (…), <u>biometric data or data on criminal convictions and offences or related security measures</u>, 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 (…)[98];

    (d)   (…);

    (e)   other <u>operations where</u> the <u>competent</u> supervisory authority <u>considers that the processing is likely to</u> **result in high degree of** <u>risks for the rights and freedoms of data subjects</u>**,** **in particular** <u>because they</u> **render the exercise by** <u>data subjects</u> **of their rights under this Regulation more difficult** (…)[99].

---

[97]   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

[98]   BE, FR, SK asked for the deletion or better definition of 'large scale'. COM referred to recital 71 and said that the intention was not to cover every camera for traffic surveillance, but only 'large scale'.

[99]   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. DE found it meaningful to have paragraph (e) because of technical and societal needs

2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board. [100]

2b. Prior to the adoption of the list the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. [101]

3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risks **referred to in paragraph 1**, the measures envisaged to address the risks[102] including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[103] taking into account the rights and legitimate interests of data subjects and other persons concerned[104].

3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment**[105]**.

---

[100] Moved from Article 34(4). BE, CZ, EE, NL 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.

[101] Moved from Article 34(5). BE, CZ, EE, NL 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.

[102] DE suggests adding 'also in view of Article 30'.

[103] NL proposes to specify this reference and refer to Articles 30, 31, 32 and 35.

[104] 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.'

[105] HU thought this should be moved to a recital.

4.   (…)[106]

5.   (…) <u>Where the processing pursuant to point (c) <u>or (e)</u> of Article 6(1) <u>has a legal basis in </u>Union law <u>or the law of the Member State to which the controller is subject</u>, <u>and such law regulates the specific processing operation or set of operations in question</u>, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[107].

6.   (…)

7.   (…)

Article 34
Prior (…) consultation[108]

1.   (…)

2.   The controller (…)[109] 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 <u>the</u> processing <u>is</u> likely to present a **very **high degree of (…) risk [110].

---

[106]   BE, FR indicated that this was a completely impractical obligation. NL and COM were in favour of maintaining it.
[107]   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.
[108]   ES, HU and UK scrutiny reservation; DE, NL and SK reservation on giving this role to DPAs, which may not be able to deal with these consultations in all cases. NL proposed to delete the entire article. FR however thought that Member States should be given the possibility to oblige controllers to inform the DPA of data breaches. See revised recital 74, which clarifies the scope of the obligation. FR and AT found Article 34 very problematic.
[109]   Deleted in view of BE, DK, FR, SE and PL reservation on reference to processor. COM reservation on deleting processor.
[110]   DE and ES proposed to exempt controllers from the obligation of a prior consultation in case they had appointed a DPO.

3.   Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 <u>would</u> not comply with this Regulation, in particular where **the** <u>risks</u> **is** insufficiently identified or mitigated, it shall <u>within a maximum period of 6 weeks following the request for consultation give advice</u> to <u>the data controller</u> (…)[111]. <u>This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay</u>[112].

4.   (…)

5.   (…)

6.   <u>When consulting the supervisory authority pursuant to paragraph 2,</u> the controller (…) shall provide the supervisory authority**,** with

   (a)   <u>where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;</u>

   (b)   <u>the purposes and means of the intended processing;</u>

   (c)   <u>the measures and safeguards provided to protect the rights and freedoms of data subject pursuant to this Regulation;</u>

   (d)   <u>where applicable , the contact details of the data protection officer;</u>

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

   (f)   any (…) <u>other</u> information <u>requested by</u> the supervisory authority (…)[113].

---

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

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

[113]   DE thought this paragraph should be deleted.

ALTERNATIVE:

2. The controller (…) shall **apply for an authorisation by** the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a **very** high degree of risk**, referred to in Article 33, paragraph 1, and these risks cannot be mitigated by reasonable measures in terms of available technology and costs of implementation to be taken by the controller**.

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

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

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

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

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

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

4. (…)

5.   (…)

6.   When **applying for an authorisation** pursuant to paragraph 2, the controller (…)
      shall provide the supervisory authority**, on request, with the data protection**
      impact assessment provided for in Article 33 and any (…)**information**
      requested by the supervisory authority (…)**..**

      ………………………………………………………………………………………….

7.   Member States shall consult the supervisory authority during the preparation[114] of a
      proposal for a legislative measure adopted by a national parliament or of a regulatory
      measure based on such a legislative measure which provide for the processing of
      personal data **that present a high degree of risk to fundamental right s and**
      freedoms of data subjects by virtue of the nature, scope or purposes of such
      processing[115]

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[116].

8.   (…)

9.   (…)

---

[114] CZ wanted clarification that this obligation does not apply to private member's bills and
       would prefer to limit this obligation to cases of high-risk processing.
[115] At the suggestion of IE this text was reinstated. COM reservation, in particular regarding
       regulatory measures: this threshold is not present in the 1995 Directive
[116] DK, NL, SE 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,[117] designate a data protection officer (…)[118].

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[119] (…).

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.

---

117 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.

118 PL suggested adding 'The controller or the processor may appoint one or more deputy data protection officers. Deputy data protection officer must fulfil conditions stipulated in art. 35 point 5 of this Regulation"

119 PL suggested adding a reference to the absence of a criminal record as a condition.

8.   The data protection officer may be <u>a staff member of</u> the controller or processor, or fulfil <u>the</u> tasks on the basis of a service contract<u>.</u>

9.   The controller or the processor shall <u>publish the</u> contact details of the data protection officer <u>and communicate these</u> to the supervisory authority (…).

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

11.   (…)

Article 36
Position of the data protection officer[120]

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 <u>referred to in Article 37 by</u> provid<u>ing</u> (…) resources necessary to carry out <u>these tasks as well as access to personal data and processing operations</u>.

<u>3.</u>   The controller or processor shall ensure that the data protection officer <u>can</u> <u>act in an independent manner</u> <u>with respect to the performance of his or her tasks</u>[121] and does not receive any instructions <u>regarding</u> the exercise of the<u>se tasks</u>. The data protection officer shall directly report to the<u> highest management level</u> of the controller or the processor.

---

[120]   UK thought articles 36 and 37 could be deleted in a pure risk-based approach.
[121]   DE, EE, ES, LV and NL pointed out that the requirement of independence was not the same for DPOs as for DPAs.

4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests[122].

Article 37

Tasks of the data protection officer

1. The **(…)** data protection officer (…) **shall have**[123] the following tasks:

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

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

   (c) (…)

   (d) (…)

   (e) (…)

---

[122] 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.

[123] NL proposal.

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

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

(h)   to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation/**authorisation** referred to in Article 34, and consult, as appropriate, on any other matter[124].

2.   (….)

2a.   The data protection officer shall perform his tasks, pursuant to the Regulation with due regard to the risks associated with the processing operations, taking into account the purpose, nature and context of the processing[125].

---

[124]   FR suggested adding an obligation to draft an annual report on his activities, but this may be too heavy an obligation.
[125]   NL proposal.

SECTION 5

CODES OF CONDUCT AND CERTIFICATION[126]

Article 38

Codes of conduct [127] [128]

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

1a. Associations and other bodies representing categories of controllers or processors[129] 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;

---

[126]   COM scrutiny reservation on Section 5.
[127]   AT, DK, FI, SK and PL scrutiny reservation. DE, FR and SI stated that this article should not apply to the public sector.
[128]   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)
[129]   LU pleaded in favour of extending this to multinational companies established in various Member states.

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

1b.   Such a code of conduct shall contain mechanisms **which enables the body referred to in paragraph 1 of article 38a to monitor compliance with its provisions**[130] 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.

---

130   IE proposal.

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

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

3.   Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, the European Data Protection Board shall submit its opinion to the Commission[131].

4.   The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union[132]. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5.   The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4[133].

---

[131]   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.
[132]   CZ, EE and FR queried what was the legal status of such approved codes of conduct and in particular their binding nature.
[133]   BG suggests deleting paragraph 4; ES suggests deleting paragraphs 4 and 5.

Article 38a

__Monitoring of codes of conduct__[134]

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body[135] which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

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

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

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

    (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 demonstrate**s** to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

---

[134]   AT, DE , DK, NL, LU, FI, PT and UK scrutiny reservation.
[135]   CZ, DK, EE, LV, 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.

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

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

5.   The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation[136].

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

---

[136]   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.

Article 39

Certification[137]

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

2.   A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 **or 51a**.

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

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

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

---

[137]   AT, DK, EE, FR, FI, PT 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 an that the DPA should be in a position to check compliance with certified data protection policies; this should be clarified in Article 53.

Article 39a

Certification body and procedure[138]

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

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

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

    (b)   it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;

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

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

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

---

[138]   AT, DK, EE, FR and PT scrutiny reservation.

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

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

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

6a.   The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

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

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

8.   The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)[139]

---

[139]   DE pleaded in favour of deleting the last two paragraphs. ES thought that this should not be left exclusively to the Commission.