Council of the European Union

Brussels, 3 July 2014
(OR. en)

11481/14

LIMITE

DATAPROTECT 99
JAI 583
MI 513
DRS 91
DAPIX 97
FREMP 136
COMIX 356
CODEC 1556

Interinstitutional File:
2012/0011 (COD)

NOTE

From:	Presidency
To:	Working Party on Information Exchange and Data Protection
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Risk based approach

1. In the course of the first examination of the proposal for a General Data Protection Regulation, several Member States voiced their disagreement with the level of prescriptiveness of a number of the proposed obligations in the draft Regulation. At the same time, some others have recalled the need to guarantee legal certainty in the proposed Regulation.

2. Following an invitation by the Cyprus Presidency to give their views on alternative ways of reducing administrative burden while maintaining the protection of individual rights, a common view emerged that the risk inherent in certain data processing operations should be a main criterion for calibrating the data protection obligations. Where the data protection risk is higher, more detailed obligations would be necessary and where it is comparably lower, the level of prescriptiveness can and should be reduced.

3. At the JHA Council meeting in December 2012, DAPIX was instructed to work on concrete proposals to implement a strengthened risk-based approach in the text of the draft Regulation. During the Irish Presidency, very substantial steps were made towards incorporating such a risk-based approach in the text of the draft Regulation, in particular in Chapter IV (Controller and Processor), and in certain articles in Chapter III (Rights of the Data Subject).

4. As a consequence amendments were made to the proposed Regulation as regards the text of Chapter IV (on the controllers' and processors' responsibility). The revised draft of this Chapter includes a 'horizontal clause' in Article 22 of the Regulation, accompanied by a risk-based redrafting of many provisions of this Chapter (especially articles 23, 26, 28, 30, 31, 33, 34 and 35). Provisions with limited value-added (articles 27 and 29) have been dropped. Equally several important articles in Chapter III, including articles 12, 14 and 15 were changed in order to ensure effective and efficient exercise of data subject rights, while improving certainty and transparency.

5. At the Council of 6-7 March 2013, there was a large agreement on the need to reduce burdens on enterprises, in particular regarding small and medium-sized enterprises (SMEs). COREPER and DAPIX were instructed to continue work on the risk-based approach, inter alia, by further developing criteria for enabling the controller and processor to distinguish risk levels and by further exploring the use of pseudonymous data as a means of calibrating controllers' and processors' data protection obligations.

6. There appeared to be a majority of Member States in favour of controllers engaging in prior consultation with the supervisory authority where their risk assessment indicates that envisaged processing operations are likely to present a high degree of risk. A large majority of Member States thought that the designation of a data protection officer should be optional rather than mandatory. There was general support for incentivising the linkage of approved codes of conduct and the use of approved data protection certification mechanisms by establishing linkages with the risk assessment process.

7. 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, it is equally clear that many Member States are of the opinion that more efforts need to be undertaken to reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach. Obviously this should be done whilst maintaining a high level of data protection.

8. To this end the Presidency is making a number if suggestions regarding further changes to Chapter IV and is inviting delegations to ask a number of questions.

9. Regarding the risk concept referred to in Article 22 and recitals 60, several delegations are of the opinion that this should be further detailed and that a description or definition of low risk should also be given. Delegations are invited to provide drafting regarding low risk situations.

10. Regarding the role of a processor, paragraph 2 of Article 26 lists, in a mandatory way, a number of obligation on the processor to be set out in a contract or other legal act binding the processor to the controller. In view of the fact that this will apply to any kind of subcontracting involving personal data, even one-off transactions with a very low risk, the mandatory character of this list has been criticised by a number of delegations for being overly prescriptive. Delegations are therefore invited to indicate whether this requirement should be made less prescriptive, and if so, how. One suggestion has been to require the setting out of these obligations only "where relevant", which would offer more flexibility, but at the same time starkly reduce legal certainty. Another possibility would be to refer to a risk criterion.

11. In Article 30, one addition is suggested in order to clarify the concept of security.

12. Data breach notification is one of the items on which the Irish Presidency succeeded to incorporate a strong risk-based approach. Delegations are invited to confirm that the current text meets their view on risk-based approach or whether they see scope for other amendments in line with the wish to have a risk-based approach[1].

13. Regarding data protection impact assessment (DPIA), the Presidency has followed a suggestion for rephrasing the reference in Article 33(2)(b) by deleting the 'large-scale' qualification but by referring instead to the legitimate expectations as a criterion allowing controllers not to have to carry out a DPIA. Thus is obvious that some controllers, by the very nature of their professional activities, (such as doctors, hospitals, attorneys, border agencies, etc.) in certain cases be expected to process sensitive data on a large scale, without this justifying a DPIA. At the same time the Presidency acknowledges that the introduction of such criterion may significantly affect legal certainty. In recital 71 and point (e) of Article 33(2), further clarifications have been suggested regarding other processing operation which warrant a DPIA.

14. At the Council meeting of 6-7 March 2013 a majority of Member States was in favour of controllers engaging in prior consultation with the supervisory authority where their risk assessment indicates that envisaged processing operations are likely to present a high degree of specific risk. 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. Delegations are therefore invited to indicate whether they think that the instrument of a prior consultation should be incentivised by any or more of the following options:
    a) prohibiting processing operations pending the opinion of the data protection authority;
    b) prohibiting processing operations for which the data protection authority has rendered a negative opinion; or

[1] In this regard see the notification mechanism set forth in Regulation 611/2013 further to directive 2002/58/EC as amended by directive 2009/136/EC, which does not envisage assessment of the risk for data subjects prior to notification to the competent authority (DPA or other).

c) providing for an administrative sanction in case of failure to consult the data protection authority.

15. The suggested clarification in Article 38(1)(f) is meant to enhance the risk-based approach by linking codes of conduct with the conditions for cross-border data flows to third countries , for the purpose of specifying the application of provisions of this Regulation.
Article 33 has also been amended to state that compliance with codes of conduct should be taken into account for the purpose of a DPIA.

16. Regarding both codes of conduct and certification, the Presidency is inviting delegations to express themselves clearly on the role data protection authorities should play. It should be clarified whether compliance with a code of conduct can be monitored only by the body currently referred to in Article 38a or also by the data protection authority. Also, it should be confirmed which body/authority issues a certification: a certification body accredited by the data protection authority or also the data protection authority itself.

17. Delegations are welcome to make any other suggestion for increasing the' risk-based in approach in (Chapter IV of) the draft Regulation with a view to finalising the discussions on this horizontal theme. The Presidency would also like to emphasise that this note does not intend to deal with all outstanding issues regarding Chapter IV, but that the Presidency will obviously return to Chapter IV at a later stage.

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. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:

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

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 ~~designation of~~ **indications provided by** a data protection officer or, where a data protection impact assessment indicates that processing operations involve a high degree of specific risks(..), **which cannot be mitigated by reasonable measures in terms of available technology and costs of implementation**, through consultation of the supervisory authority prior to the processing.

59) 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.

60) 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.

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

The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance of the controller.

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated by means of adherence of the processor to a code of conduct or a certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted **either directly** by the Commission or by a supervisory authority in accordance with the consistency mechanism and **then** adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.

64) (…)

64a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to present specific risks 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 specific 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 in any case to accidental or unauthorised access, destruction, loss, modification or dissemination of personal data[2].**

[2] This is meant to ensure that a minimum level of security measures is taken into consideration in any case. The list of specific risks is taken from Convention 108/1981

67) A personal data breach may, if not addressed in an adequate and timely manner, result in severe material or moral harm to individuals such as loss of control over their personal data or the 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. Therefore, as soon as the controller becomes aware that (…). a personal data breach has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals **whose personal rights and freedoms** could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. **(…)**. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example (…) **the need** to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

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.

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 and using pseudonymous 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 specific risks, taking into account the nature, scope and purposes of the processing and the sources of the risks, which should include in particular the envisaged measures, safeguards and mechanisms **for mitigating those risks and** for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

71) This should in particular apply to newly established large scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects**, as well as to processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where legitimate expectations are not met, for example owing to the context of the processing operation[3].**

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.

[3] Further to proposal by DE.

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

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

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

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.

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[4]

SECTION 1
GENERAL OBLIGATIONS

Article 22

Obligations of the controller[5]

1. Taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects[6], the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation[7].

---

4 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).

5 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.

6 Several delegations stressed that the risk concept should be further detailed: DE, ES, HU, NL, PT, FI and RO. DE, ES and SE pointed out a description or definition of low risk was missing.

7 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. (…)[8]

2a. Where proportionate in relation to the processing activities9, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller10.

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 (….)[11].

3. (…)

4. (…)

[8] PL asked for the reinstatement of this paragraph.

[9] HU 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.

[10] UK thought this was too complicated. ES thought the concept of 'appropriate data protection policies' was too vague.

[11] Reference to auditors deleted in view of the remarks made by CZ, ES and IT.

Article 23

Data protection by design and by default[12]

1. Having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall (…), implement (…) technical and organisational measures appropriate to the processing activity being carried on and its objectives, including pseudonymisation of personal data, in such a way that the processing will meet the requirements of this Regulation and (…) protect the rights of (…) data subjects.[13]

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are not excessive[14] for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals[15].

---

12 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.

13 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.

14 ES proposed to replace 'necessary' by 'not excessive in quantity'.

15 DE, IT 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 [16]

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[17] 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.

---

16 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.

17 BE proposed adding: 'The arrangement shall duly reflect the joint controllers' respective effective roles vis-à-vis data subjects. The arrangement shall designate the supervisory authority in accordance with Article 51. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.' 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[18] 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[19]

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union[20].

[18] 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.

[19] 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.

[20] 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[21]; or

(b) an enterprise employing fewer than 250 persons unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing[22]; or

(c) a public authority or body[23].

(d) (…)[24]

[21] BE, DE, IT, 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.

[22] 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. FR thought that the risk-criterion should be described in a uniform manner throughout the Regulation.

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

[24] DE and SK thought that this scenario was not covered by Article 3(2). There appears to be no more need for this subparagraph now in view of the revised recital 23.

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[25].

3a. The representative shall be mandated by[26] 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.

[25] 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.

[26] BE proposed to state 'is liable'.

Article 26

Processor[27]

1. (…)[28] The controller shall use only processors providing sufficient guarantees[29] to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…)[30].

2. The carrying out of processing by a processor shall be governed by a contract or other legal act[31] binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects (…)and stipulating, in particular that the processor shall:

---

27 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) in a horizontal way, by including, inter alia, the DPA powers.

28 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.

29 BE, DK and HR thought the 'sufficient guarantees' should be detailed.

30 The latter part of the article was deleted as it added nothing substantial: IE, NL and SE. DE thought it could be put in a separate sentence.

31 HR wanted to know what was meant by an 'other legal act'. SE thought a recital should clarify it could cover Member State legislation. AT suggested that the details referred to for the contract should also apply to 'other legal act'.

(a) process the personal data only on instructions from the controller (…)[32], unless required to do so by Union or Member State law to which the processor is subject**;** in such a case, the processor shall inform the controller of that legal requirement, unless that law prohibits such information on important grounds of public interest[33];

(b) (…)

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

(d) [34]respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller[35];

(e) as far as (…) possible, taking into account the nature of the processing[36], 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;

---

32 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.

33 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.

34 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.

35 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.

36 FR thought this was unclear and should possibly replaced by a reference to risk . IT thought different types of risk could be referred to here.

(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services[37][38] 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[39];

(h) make available to the controller (…) all information[40] necessary to demonstrate compliance with the obligations laid down in this Article.

2a. Where a processor enlists by way of a contract or other legal act another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. 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[41].

---

37 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.

38 FR, ES and NL request that there should be an obligation to return the data.

39 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'.

40 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.

41 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.

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[42].

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[43], 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[44].

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) [45].

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.

---

42 BE 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 be 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.

43 ES suggestion.

44 IE reservation.

45 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).

4. (…)

5. (…)[46]

Article 27

Processing under the authority of the controller and processor

(…) [47]

Article 28

Records[48] of categories of personal data processing activities [49]

1. Each controller (…)[50] and, if any, the controller's representative, shall maintain a record of all categories of personal data processing activities under its responsibility[51]. [52]This record shall contain (…) the following information:

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

---

46 COM reservation on deletion.

47 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.

48 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.

49 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.

50 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.

51 FR thought it should be specified for how long the documentation needed to be kept.

52 ES proposed to insert a sentence along the following lines: 'Controllers that do not have a data protection officer or sufficient certificate in force, shall have the legally established documentation form with regard to all processing operations carried out under their responsibility'. 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.

(b) (…)

(c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f)[53];

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

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

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation (…)[54];

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

(h) (…)

2a. Each processor[55] 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;

---

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

54 UK reservation.

55 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.

(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[56].

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

(a) (…)[57]

(b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing[58]; or

(c) categories of processing activities which[59] by virtue of the nature, scope or purposes of the processing are unlikely to represent specific risks for the rights and freedoms of data subjects.

5. (…)

---

56 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.

57 COM reservation on deletion.

58 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).

59 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.

6. (…)

Article 29

Co-operation with the supervisory authority

(…)[60]

[60] PT and ES scrutiny reservation on deletion.

SECTION 2

DATA SECURITY

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor[61] shall implement appropriate technical and organisational measures, including pseudonymisation of personal data to ensure a level of security appropriate to these risks.

1a. In assessing the level of security account shall be taken in particular of the risks arising from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[62].

2. (…)

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

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

---

61 Several delegations thought that the controller should have the main responsibility (NO, NL, RO, UK).

62 It would appear to be appropriate to ensure that security measures are taken in any case, i.e. that no processing of personal data may ever go without security measures. This list is taken from Convention 108/1981, Art. 7.

3. (…)

4. (…)

Article 31

Notification of a personal data breach to the supervisory authority[63]

1. In the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects[64], 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)[65].

2. (…) The processor shall alert and inform the controller without undue delay after becoming aware of a personal data breach[66] [67].

---

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

64 BE suggested adding: 'or creates a risk for the data subjects'.

65 BE thought that also point (a) of Article 32(3) should be added here.

66 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.

67 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.

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

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

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

(c) (…)

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

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

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

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

4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, comprising the facts surrounding the breach, its effects and the remedial action taken[68].This documentation must enable the supervisory authority to verify compliance with this Article. (…).

[68] AT, LU and FR queried what was the retention period for this documentation. IT proposed to insert a reference to the estimated severity of the remedial action taken.

5. (…)

[6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[69]]

Article 32

Communication of a personal data breach to the data subject[70]

1. When the personal data breach is likely to severely affect the rights and freedoms of the data subject[71], the controller shall (…)[72] communicate[73] 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[74] 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).

---

69 BE, DE, IT, LT, RO and UK pleaded for the deletion of paragraph 6.

70 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.

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

72 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'

73 PL suggested specifying this could be done either in paper or electronic form.

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

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

a. the controller (…)[75] has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, in particular those that[76] render the data unintelligible to any person who is not authorised to access it, such as encryption **(…)**; or

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

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

d. it would adversely affect a substantial public interest.

4. (…)

5. (…)

[6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).[77]]

---

75 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.

76 BE proposed 'have the purpose'.

77 BE, CZ, DK, DE, ES, PL and UK pleaded for the deletion of paragraph 6.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33

Data protection impact assessment [78]

1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present **high**[79] risks[80] for the rights and freedoms of data subjects[81], the controller **(…)**[82] shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)[83]. **(…).** [84]

1a. The controller shall seek the advice of the data protection officer, where applicable[85], when carrying a data protection impact assessment.

---

78 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.

79 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. UK suggested to define *specific risk.*

80 DE thought that the risk-based approach needed further study. IE wanted to look at risk isolated from how risk was dealt with in other parts of the Chapter and their consistency; *e.g.* when was the impact assessment carried out, maybe there was no DPO in place when the impact assessment was carried out.

81 BE and RO scrutiny reservation.

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

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

84 Text deleted because this obligation is already set forth in Article 26(2), letter f).

85 PL asked whether *where applicable* meant that the controller always must ask advice of the DPO.

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

[(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions[86] are based that produce legal effects concerning data subjects or severely affect data subjects[87];]

(b) processing of **[special categories of personal data under Article 9(1), data on children, biometric data]** or **data on** criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals **(…)**[88] [**and legitimate expectations of the data subject are not met, for example owing to the context of the processing operation]**;

(c) monitoring publicly accessible areas *on a large scale*, especially when using optic-electronic devices (…)[89];

(d) **(…)**[90];

---

86 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.

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

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

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

90 This paragraph is unnecessary given that it is already covered by letter (b) above.

(e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects[**, or because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale]**[91].

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. [92]

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. [93]

---

91 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

92 New paragraph 2a moved from Article 34(4) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

93 New paragraph 2b moved from Article 34(5) and aligned with revised point (e) of paragraph 2. BE, CZ, EE and DE reservation.

3. The assessment shall contain at least a general description of the envisaged processing operations, an **evaluation** of the risks for rights and freedoms of data subjects, the measures envisaged to address the risks[94] **including** safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation[95] taking into account the rights and legitimate interests of data subjects and other persons concerned[96].

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

4. (…)[97]

---

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

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

96 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.'

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

5. **(…)** [98]**W**here the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, **and such law regulates the specific processing operation or set of operations in question,** paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities[99].

6. (…)

7. (…)

Article 34

Prior (…) consultation[100]

1. (…)

---

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

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

100 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..

2. The controller (…)[101] shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a high degree of specific risks[102] [103]. **(…)** [104]

3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller (…)[105]. 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[106].

4. (…)

5. (…)[107]

---

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

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

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

104 Text deleted because this obligation is already set forth in Article 26(2), letter f).

105 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).

106 ES, NL and SI scrutiny reservation. FR, supported by IT, 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.

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

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

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

(b) the purposes and means of the intended processing;

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

(d) where applicable , the contact details of the data protection officer;

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

(f) any (…) other information requested by the supervisory authority (…).[108].

7. Member States shall consult the supervisory authority during the preparation[109] 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 (…). **[110]**

108 DE thought this paragraph should be deleted.

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

110 IE noticed that text had been dropped from paragraph 7; the interpretation could be too broad; as it now reads every municipality could be obliged to consult the SA for any regulatory measure. Therefore IE considered it necessary with guidance in a recital.

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[111].

8. (…)

9. (…)

[111] 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,[112] designate a data protection officer (…)[113].

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[114] (…).

6. (…)

---

112 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.

113 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"

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

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

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

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

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

11. (…)

Article 36

Position of the data protection officer[115]

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

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

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

3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks[116] and does not receive any instructions regarding the exercise of these tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests[117].

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer (…) with 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;

---

116 DE, EE, ES, LV and NL pointed out that the requirement of independence was not the same for DPOs as for DPAs.

117 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.

(c) (…)

(d) (…)

(e) (…)

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

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

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter[118].

2. (….)

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

SECTION 5

CODES OF CONDUCT AND CERTIFICATION[119]

Article 38

Codes of conduct [120] [121]

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[122] 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;

---

[119] COM scrutiny reservation on Section 5.

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

[121] 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)

[122] 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), letter d**[123].

1b. Such a code of conduct shall contain mechanisms for monitoring and ensuring compliance with it 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.

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[124] give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.

---

123 NL queried whether this also covered the transfer to processors in 3rd countries.

124 Further to CY, FR, IT, LU, LV and PT suggestion.

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[125] (…).

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[126]. 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[127].

---

125 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.

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

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

Article 38a

Monitoring (…) of codes of conduct[128]

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[129] 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.

---

128 AT, DE , DK, NL, LU, FI, ,IT , PT and UK scrutiny reservation.

129 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**130**.

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

130 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[131]

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.

[2a. The certification shall be issued by the competent supervisory authority, which may be supported in this task by accredited bodies under Article 39a.]

3. The controller or processor which submits its processing to the certification mechanism shall provide [**the competent supervisory authority or, where applicable, the]** body referred to in Article 39a (1) 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 [**supervisory authority , which may be supported in this task by an accredited]** body referred to in paragraph 1 of Article 39a ~~or by the competent supervisory authority~~. It shall be withdrawn [**by the supervisory authority]** where the requirements for the certification are not or no longer met.

---

131 AT, DK, EE, FR, FI , IT , 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[132]

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.

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. (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.

[132] AT, DK, EE, FR, IT 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**, **if so instructed by the competent supervisory authority,]** without prejudice to the responsibility of the controller or processor for compliance with this Regulation.

4a. **(…)**

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]. **[The European Data Protection Board shall give an opinion to the Commission on these criteria and requirements]**.

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)[133]

---

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