NOKIA
Connecting People

November 6, 2012

Set of Amendments implementing the Accountability Principle into Law

Article 22 (Responsibility of the controller)	
Commission proposal	**Proposed amendment**
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	***1. Having regard to the state of the art, the nature of personal data processing and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself, the controller and processor shall implement appropriate and demonstrable technical and organizational measures in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject by design.*** ***2. Such measures include, without limitation,*** ***(a) Sufficiently independent management oversight of processing of personal data to ensure the existence and effectiveness of the technical and organizational measures;*** ***(b) Existence of proper policies, instructions or other guidelines to guide data processing needed to comply with the Regulation as well as procedures and enforcement to make such guidelines effective;*** ***(c) Existence of proper planning procedures to ensure compliance and to address potentially risky processing of personal data prior to the commencement of the processing;***

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.	***(d) Existence of appropriate documentation of data processing to enable compliance with the obligations arising from the Regulation;*** ***(e) Existence of adequately skilled data protection organization or data protection officer or other staff supported with adequate resources to oversee implementation of measures defined in this article and to monitor compliance with this Regulation, having particular regard to ensuring sufficient organizational independence of such data protection officer or other staff to prevent inappropriate conflicts of interest. Such a function may be fulfilled by way of a service contract;*** ***(f) Existence of proper awareness and training of the staff participating in data processing and decisions thereto of the obligations arising from this Regulation;*** ***3. Upon request by the competent data protection authority, the controller or processor shall demonstrate the existence of technical and organizational measures.*** ***4. Group of undertakings may apply joint technical and organizational measures to meet its obligations arising from the Regulation.*** ***5. This article does not apply to a natural person processing personal data without commercial interest.***

NOKIA
Connecting People

Justification

We believe all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures to ensure compliance with the Regulation. Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines[1] and APEC Privacy Framework[2] and in the laws of for example Canada and Mexico.

Implementing such Accountability concept in the Data Protection Regulation instead of opting for the antiquated prescriptive and straight-jacked set of detailed and prescriptive compliance requirements as currently proposed would in practice allow controllers, processors and DPAs to focus their attention on what is really necessary to deliver optimal data protection. This will result in improved data protection and avoid unnecessary burden for all parties involved.

Amendment

Art 23 (Data Protection by Design/Default)	
Commission proposal	**Proposed amendment**
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. Having regard to the state of the art ~~***and,***~~ the cost of implementation ***and international best practices***, ***appropriate measures and procedures shall be implemented where technically feasible to ensure the processing operation meets***, ~~***the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet***~~ the requirements of this Regulation and ensure***s*** the protection of the rights of the data subject.

[1] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[2] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. ***Such measures and procedures shall:*** (a) ***follow the principle of technology, service and business model neutrality*** (b) ***be based on global industry-led efforts and best practices*** ***(c) be flexible based on an entities' business model, size, and level of interaction with personal data*** ***(d) take due account of existing technical standards and regulations in the area of public safety and security*** (e) ***take due account of international developments*** ***~~2.The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.~~***
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design	3. ***In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market***

requirements applicable across sectors, products and services.	***and the free circulation of such equipment in and between Member States.*** ~~***The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.***~~
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~***4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Justification

Privacy by design is an important concept. Having in place technical and organizational measures helps to ensure data protection is at the heart of privacy by design. However, art. 23 appears to be a generic definition, while other articles include further and more detailed data protection by design –type of obligations. For example, the current proposed art. 23 to a large extent overlaps with art. 22 and art. 5 c). In addition, some of the needed technical and organizational measures are actually those defined in, for example, in the following articles: Art. 26 (processor agreements), art. 28 (documentation), art. 30 (security), art. 33 (data protection impact assessment) and art. 35 (data protection officer). We believe that such repetition is likely to lead to confusion and does not add value. A better result is achieved through an improved art. 22 as suggested by amendment 30 introducing the Accountability concept and by adding the last sentence of proposed art. 23.2 to art. 5 b) (principles relating to personal data processing).

Amendment

Article 28 (documentation)	
Commission proposal	**Proposed amendment**
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller ~~***and processor***~~ and, if any, the controller's representative, shall maintain documentation of ~~***all***~~ ***the main categories of*** processing ~~***operations***~~ under its responsibility.
2. The documentation shall contain at least the following information:	2. **Such** documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;	(b) the name and contact details of the data protection **organization or data protection** officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	(c) the **generic** purposes of the processing ~~**including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);**~~
(d) a description of categories of data subjects and of the categories of personal data relating to them;	(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	(e) the categories of recipients of the personal data, ~~**including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;**~~

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	(f) where applicable, transfers of **personal** data to a third country or an international organisation, and, in case of transfers referred to in point (h) of Article 44(1), a reference to safeguards employed;
(g) a general indication of the time limits for erasure of the different categories of data;	(g) a general indication of the time limits for erasure **or data retention policy applicable to** the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).	(h) ~~**the description of the mechanisms referred to in Article 22(3).**~~
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	3. The controller ~~***and the processor***~~ and, if any, the controller's representative, shall make the documentation available, on ***the basis of a*** request ***outlining the reasons for requiring access to the documents***, to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers ~~***and processors***~~: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation	5~~***. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the***~~

referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	~~***responsibilities of the controller and the processor and, if any, the controller's representative.***~~
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. **To ensure harmonized requirements within Europe, t**he Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Effective data protection requires that organizations have a sufficiently documented understanding of their data processing activities. The documentation requirement in art 28.2 appears to largely duplicate the notification provisions in art. 14, is unnecessarily burdensome and even empowers the Commission to provide even more detailed documentation requirements. Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations and the lead DPA to effectively enforce the Regulation. Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. It should be left to the controllers and processors – in agreement with the lead DPA - based on the Accountability principle to determine which documentation is adequate and best suited for specific processing activities to comply with this Regulation and achieve the desired protection. Finally, art. 28.3 is unnecessary because of art. 29.

Amendment

Article 33 (Data protection impact assessment)	
Commission proposal	**Proposed amendment**
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact	~~**1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the**~~

of the envisaged processing operations on the protection of personal data.	~~protection of personal data.~~
2. The following processing operations in particular present specific risks referred to in paragraph 1:	~~2. The following processing operations in particular present specific risks referred to in paragraph 1:~~
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	~~(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;~~
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	~~(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;~~
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;	~~(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;~~
(d) personal data in large scale filing systems on children, genetic data or biometric data;	~~(d) personal data in large scale filing systems on children, genetic data or biometric data;~~
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	~~(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).~~
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data	~~*3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data*~~

subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.	~~*subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.*~~
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	~~*4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.*~~
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	~~**5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.**~~
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	~~*6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.*~~
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall	~~*7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those*~~

be adopted in accordance with the examination procedure referred to in Article 87(2).	~~***implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Justification

The DPIA obligation is seriously flawed as it is currently proposed. The approach to single out certain types of processing, brand them as risky and treat them differently from supposedly non-risky processing is dangerous and will not produce the desired results. We believe all processing of personal data should be planned appropriately prior to commencing the processing to ensure compliance with the Regulation. Organizations should be held accountable for applying risk identification and mitigation planning methodologies that are appropriate for the processing at hand. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing. Some of the activities listed in article 33 are standard processing for which such an assessment should not need to be submitted to a DPA for prior authorization or consultation. In the current online reality, processing of e.g. location data, user segmentation and other such practices described as potentially risky in the proposal, are the norm rather than exception and do not necessarily pose any significant risk to individuals.

Furthermore, DPIA's are only one specific method, among others (constantly evolving methodologies), to achieve the ultimate objective of ensuring that risks to privacy have been identified and proper mitigations planned in a timely fashion. It therefore does not make sense to regulate DPIAs in a strict manner while ignoring the broader picture of the risk assessing and mitigation toolkit. Risk assessment and mitigation should be the responsibility of the controller according to the Accountability Principle implemented via the amendment to article 22.

Amendment

Article 34 (Prior authorisation and prior consultation)	
Commission proposal	**Proposed amendment**
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor	1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor

adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.	adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.
2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	(a) ~~**a data protection impact assessment *as provided for in* Article 33 indicates that**~~ ***the processing is based on point (e) or (f) of Article 6(1) and the*** processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks~~***; or***~~
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	~~***(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.***~~
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.	3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance. ***Such a decision shall be***

	subject to appeal in a competent court and it may not be enforceable while being appealed unless the processing would result in immediate serious harm suffered by data subjects.
4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to ~~**point (b) of**~~ paragraph 2. ***The following processing operations are likely to present specific risks:*** ***(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects <u>that gravely and adversely affect the individual's fundamental rights</u>;*** ***(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*** ***(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;*** ***(d) personal data in large scale filing systems on children, genetic data or***

	biometric data; ***The supervisory authority shall communicate those lists to the European Data Protection Board.***
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	~~***5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.***~~
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, ***on request***, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	~~**6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33, and with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.**~~
7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	~~***7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.***~~

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.	***~~8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.~~***
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	9. The Commission may set out ***non mandatory*** standard forms and procedures for prior authorisations ***~~and consultations~~*** referred to in paragraph***~~s~~*** 1 ***~~and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6~~***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Mandatory prior consultation should take place between supervisory authorities and data controllers and processors where needed, i.e. in exceptional cases which present specific risks and where the processing is not being carried out based on the data subject's consent but on other grounds (contract, legal obligation). In all other cases, the supervisory authorities should concentrate their limited resources on ensuring an effective and consistent ('ex-post') enforcement of the law, similar to other regulatory areas, including health and safety regulations. See also the recommendation of the Article 29 Working Party in its Opinion 3/2010 paragraph 63.

Amendment

Article 35 (Designation of Data Protection Officer)	
Commission proposal	**Proposed amendment**
1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority	1. The controller and the processor shall designate a **data protection organization or** data protection officer in any case where: (a) the processing is carried

or body; or	out by a public authority or body; or
(b) the processing is carried out by an enterprise employing 250 persons or more; or	(b) the processing is carried out by an enterprise employing 250 persons or more; or
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.
2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.
3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, the data protection **organization or data protection** officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.
5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of	5. The controller or processor shall designate the data protection **organization or data protection**

	data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.		officer 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. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.
6.	The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.		6. The controller or the processor shall ensure that any other professional duties of the data protection **organization or data protection** officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.
7.	The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.		8. The data protection officer may be employed by the controller or processor, or fulfill his or her tasks on the basis of a service contract. 9. The controller or the processor shall communicate the contact details of the data protection organization or data protection officer to the supervisory authority ***~~and to the public.~~***
8.	The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.		10. Data subjects shall have the right to contact the **data protection organization** on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.
9.	The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to		***~~11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core~~***

the public. 10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation. 11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	~~***activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.***~~

Justitfication

There are clear benefits in having in place roles and responsibilities to ensure compliance. The proposal, however, appears overly detailed in describing the tasks of a data protection officer and it also fails to recognize that also other organizational structures may result in equally or even more effective data protection. Here again it will be much more effective to take the Accountability principle into account and legislate accordingly. In larger organizations it is not reasonable to expect that a single data protection officer would be involved in all issues relating to the protection of personal data. Often in larger organizations the data protection roles and responsibilities, ranging from requirements setting, implementation, training and awareness, incident response and oversight and reporting are rightfully decentralized across the organizations, while being bound together by a comprehensive data protection program. Without senior management support and a systematic management approach, it is unlikely that such a mandatory advisory and monitoring role envisaged by the proposal will lead to desired outcomes.

Some requirements for data protection officers in the proposal may even be counterproductive. For example, creating a two year protected term in form of a job guarantee for a data protection officer creates incentives to outsource the role to an external service provider to balance the risk of an unsuccessful recruitment. As in-depth knowledge of the organization is often a prerequisite for successful data protection, outsourcing can hardly be seen as a desired outcome in all cases. Also, some organizational flexibility will lead to a better organisation of the data protection resources: often, a member of the organizations senior management responsible according to the Accountability principle (and being an element of it) will achieve better data protection results than a data protection officer with a rather procedural role.

Amendment

Article 36 (position of the data protection officer)	
Commission proposal	**Proposed amendment**
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.	1. The controller or the processor shall ensure that the data protection **organization or data protection** officer is properly and in a timely manner involved in all ***significant*** issues which relate to the protection of personal data.
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	2. ~~***The controller or processor shall ensure that t***~~***T***he data protection organization or data protection officer***s shall*** perform~~***s the***~~ ***their*** duties and tasks independently ~~***and does not receive any instructions as regards the exercise of the function***~~. ~~***The data protection officer shall directly report to the management of the controller or the processor.***~~
3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	3. The controller or the processor shall support the data protection organization or data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Justification

It is not possible for a company to ensure that someone act "independently" just as much as it is impossible for a company to ensure that someone act honestly. Instead, this should be an obligation on the DPO.

Amendment

Article 37 (Tasks of the **data protection organization or** data protection officer)	
Commission proposal	**Proposed amendment**
1. The controller or the processor shall entrust the data protection officer at least with the following tasks: a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received; b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits; c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	1. The controller or the processor shall entrust the **data protection organization or** data protection officer at least with the following tasks: a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation ~~and to document this activity and the responses received;~~ b) ***to develop, support and monitor the implementation of measures referred to in Article 22, ~~in particular~~*** ~~to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;~~ c) ***to monitor compliance with the Regulation.*** ~~the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects~~

	~~and their requests in exercising their rights under this Regulation;~~

Justification

In today's organizational reality a lot of everyday advice is given over the phone, in meetings, through email or instant messaging. Having an obligation to systematically document one's everyday interaction with supported business operations would generate a massive and disproportionate administrative burden. However, actual privacy impact assessments and similarly structured privacy reviews need to be documented.

It should be up to the organization to define how they decide to organize their data protection organization and business in general. The proposed regulation appears to envision a centralized organization with full and sole control over its resources and organization, which is just one approach to reach compliance.